Multiple Domain Solution (MDS) For Single-Information-Domain Periods Processing Hosts Protection Profile

Draft

Version 0.1

12 September 2000

Prepared By:
Michael E. Herrera, AT&T
Michael A. McEvilley, Mitretek Systems
Ella T. Miller, ACS Defense, Inc.
Thomas A. Panfil, NSA

Foreword

The National Security Agency, as part of its program to architect secure, adaptable, and interoperable information assurance systems in compliance with open standards, issues this publication, Multiple Domain Solution (MDS) Protection Profile.

The base set of requirements used in this protection profile are taken from the "Common Criteria (CC) for the Information Technology Security Evaluations, Version 2.1". Further information, including the status and updates of the CC can be found on the Internet at "http:/cscr.nist.gov/cc/pp/pplist.html". Comments concerning this profile should be directed to:

Michael Herrera, GRCI (Team Lead)
Michael McEvilley, Mitretek Systems
Ella Miller, ACS Defense, Inc.
Thomas A. Panfil, NSA

Revision History

VERSION	EDITION	DATE	CHANGE PAGES	REASON
0.1	Draft	September 12,2000	None	Initial Issue

Table Of Contents

1 Introduction

1.1 Protection Profile Identification

Title: Multiple Domain Isolation Solution For Single-Information-Domain at a Time Periods Processing Hosts Protection Profile

Authors: NSA

Vetting Status: TBD

CC Version: 2.1

General Status:

Registration: TBD

Keywords: Information Flow Control, Data Isolation, Periods Processing, Information Domain, Virtual Private Network (VPN), Data Encryption

Assurance Level: EAL 4+

1.2 Protection Profile Overview

This Protection Profile (PP) specifies the minimum set of security requirements that describe a multiple domain operational capability. This capability provides an individual authorized for access to multiple domains the ability to access those domains from a single computing device, one domain at a time, through a single common network. This solution defined by this profile is based on a strongly authenticated application of cryptographic services to enforce organizationally defined domain isolation security policy.

This solution defined by this profile is intended to help address the issues that result from the current practice of allocating multiple sets of dedicated computing resources for use in distinct information domain contexts. These issues include the costs associated with equipment acquisition, operation and maintenance, the resulting ineffective use of available workspace, and the resulting impact on personnel and operational policies and practices.

The capability described by this profile is targeted at organizations that employ COTS hosts as the computing platform for access to information domains. These hosts may be employed as either user workstations or server class processing resources. These hosts are based upon either COTS operating systems with no formally evaluated level of trust or COTS operating systems with a level of trust established but without information flow control policy enforcement capabilities. Without the ability to enforce an information flow control policy (such as

Mandatory Access Controls based upon security labels), *periods processing* of the COTS computing platform (i.e, host) must be performed manually by users to ensure that domain information is not leaked across domains.

The combination of manual periods processing of the COTS host and domain information flow enforcement mechanisms ensures a secure sequence of state transitions between domain contexts within the host, and provides an operational capability that is secure and a cost-effective alternative to existing multiply instantiated resource system implementations.

1.2.1 Summary of Capabilities

The minimum high-level capabilities of a product that is compliant with this profile are stated below. Detailed discussion, additional information and a description of the TOE in the context of specific application scenarios can be found in Section 3 of this profile.

A compliant TOE provides the following capabilities:

- The isolation of information to prevent it from crossing domain boundaries as defined by information flow and/or access control policies
- The strong authentication of individuals wishing to participate in a domain, and prevention of an individual participating in multiple domains simultaneously from a single host.
- The enforcement of a *Domain Information Flow Policy (DIFP)* to ensure the containment of all information within its defined domain.
- Application of cryptography services for domain separation and information integrity and confidentiality
- Self-protection to ensure the integrity of the security-enforcing functions
- Management functions to support secure administration and operation
- Audit event generation, storage and review

The profile has been developed in accordance with the *Common Criteria for Information Technology Security Evaluation (CC), Version 2.1.*

1.3 Document Organization

The MDS PP is organized as follows:

Section 1 provides a PP Introduction and establishes the context for this PP.

Section 2 provides the conventions, (.e.g., labels, component operations, etc.), and terminology used within this PP.

Section 3 defines the TOE Description.

Section 4 contains the TOE Security Environment. This section defines the intended operating environment of the TOE through a related set of assumptions, threats and Organizational Security Policy (OSP) statements.

Section 5 provides the security objectives that support the assumptions and policies, as well as, counters the threats identified in the security environment.

Section 6 provides the security functional and assurance requirements that support the security objectives.

Section 7 provides the rationale to explicitly demonstrate that the security objectives satisfy the policies, assumptions and threats. This section also explains how the sets of requirements satisfy the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective.

Appendix A provides the concept of operations of the use-cases for employment of the TOE.

Appendix B provides the list of acronyms used within the PP.

Appendix C provides the list of reference documentation used to complete this PP.

2 Conventions and Terminology

2.1 Conventions

This profile is organized based on Annex B of Part 1 of the Common Criteria (CC). This section identifies the naming conventions or other unique terms and conventions that are used within this profile.

2.1.1 Labels

The following conventions are to aid in the referencing and understanding of assumptions, threats, policies, and objectives used throughout this profile:

Labeling Convention	**Reference Category**
A.<*name*>	Assumption
T.<*name*>	Threat
P.<*name*>	Organizational Security Policy (OSP)
O.<*name*>	Objective allocated to the TOE
OE.<*name*>	Objective allocated to the non-IT environment of the TOE
OIE.<*name*>	Objective allocated to the IT environment of the TOE

Table 2. Labeling Conventions

2.1.2 Component Operations

The notation, formatting, and conventions used in this PP are largely consistent with those used in Version 2.1 of the CC. Selected presentation choices are discussed here to aid the PP reader. Paragraph 2.1.4 of Part 2 of the CC identifies the following operations that are performed on functional requirements: *assignment*, *selection*, *iteration* and *refinement*. Each of these operations is discussed below.

2.1.2.1 Assignment and Selection

The assignment operation is used to assign a specific value to an unspecified parameter. The selection operation is used to select one or more options provided by the CC in stating a requirement. Completed assignment and selection operations are denoted by *italicized text*. Whenever an assignment or selection operation is left incomplete, the required operation is denoted either by the text "*ST writer-provided assignment*" or by "*ST writer-provided selection*" respectively. These incomplete operations, along with their required parameters, appear in ***bold italicized** text*.

2.1.2.2 Iteration

Iteration of a component is employed to apply the requirements specified by its elements multiple times to convey allocations of capabilities to partitions of the TOE, to partitions of users and administrators, or to any other partitioning perspective necessary to clearly and accurately state the requirements levied on the TOE.

The use of iteration is identified in both the component and element identifiers. At the component level, the use of iteration is identified by appending a period and an iteration to the CC-defined component name (e.g., FIA_UAU.2.1). At the element level, the use of iteration is identified by appending a plus sign and an iteration number to the CC-defined element name (e.g., FIA_UAU.2.1+1).

2.1.2.3 Refinement

The refinement operation is used to provide an elaboration of an existing CC element to explicitly meet stated objectives. Refinement of elements is denoted by **bold** text.

2.1.3 Application Notes

Application Notes are provided to clarify the intent, identify implementation choices, or define other criteria for the elements associated with a component. Application notes, where used, follow their respective component.

2.2 Terminology

This profile uses a number of terms in specific senses. The definitions of the terms that are used throughout this profile are as follows:

User: Individual or IT process acting on behalf of an individual.

Periods Processing: A manner of operating an IT system whereby the security mode of operation is established for an interval of time (i.e., the period) and then changed for an interval of time. A period extends from any secure initialization of the IT system to the completion of the purging of sensitive data handled by the IT system during this period.

Domain Information Flow Policy (DIFP): information flow policy enforced by the MDS.

Personality: an instance of the DIFP.

Individual – One or more personalities may be allocated to each individual authorized to participate in domains.

TOE – One or more personalities may be allocated to each TOE instance.

Profile: one or more domain information personalities.

Domain: The unique information context in which an IT system is operating and/or in which the user may operate (e.g communities of interest, classification levels and compartments).

Domain Participation Authentication Policy (DPAP): authentication policy enforced by the MDS. It defines the criteria (attributes for users, boot devices, credentials, etc) used during the authentication process resulting in a grant/deny permission for domain participation.

3 Target of Evaluation (TOE) Description

The TOE is envisioned to be packaged as a product that may consist of multiple physical components integrated in a manner that meets the objectives and requirements defined in this profile. At the highest level of abstraction, the TOE is specified to provide the following capabilities:

- Provide for the **isolation of network information flows** through the enforcement of domain-specific information flow control policies
- Provide the necessary **controls to invoke TOE services and to securely administer and operate the TOE**

It is anticipated that these capabilities may be successfully and effectively implemented through a variety of combinations of physical components and packaging, and of the allocation of functionality to hardware, software, and firmware. This profile intentionally makes very few assumptions for such design and implementation decisions, and levies few constraints that drive a particular design solution.

Since the TOE may be comprised of multiple distinct *physical* components operating as a single *logical* whole, it is necessary to have a well-defined and appropriately partitioned abstraction of the physical components into logical functional components. The definition, partitioning, and allocation of these logical components are not meant to imply an intended physical relationship or combination of physical devices. They are provided to make it possible for this profile to clearly articulate the TOE in terms of objectives, requirements, and rationale in an implementation independent manner. For the cases where a specific implementation is desired, this profile clearly establishes requirements that describe the details of that implementation. The as-built definition and allocation of functional requirements to components or other physical entities is left to the discretion of the Security Target/TOE developer. Furthermore, it is the responsibility of the Security Target developer to develop a correct and proper abstraction of this profile and to provide the analysis and supporting evidence to substantiate any conformance claims to this profile.

3.1 TOE Definition

This profile defines and addresses the TOE in terms of logically related capability components, hereafter referred to as components. The use of the term **TOE** means all defined components. The term TOE Security Functions **(TSF)** means all the TSF of the defined components of the TOE. The use of the term ***Component*-TSF** addresses only the TSF for that named component of the TOE.

The TOE consists of the five major components: Network, Host, Management, User, and Credential Input. These components are defined as follows:

- **Network Component.** The network component provides the interface between the Host Component and the communications media. The network component is envisioned to be a physical card or other hardware device with associated firmware and/or software. No assumptions are made regarding the integration of the network component with the host component. That is, the network component may be an inseparable part of the Host component (i.e., part of the host motherboard), it may be a device plugged into the Host component and enclosed within the physical casing of the Host component (i.e., removable card), or it may be a device external to the Host component connected between the Host component and the network.

- **Host Component.** The host component is a computing device such as a single-user or multi-user workstation, or an information server (e.g., file, database, web, or email). The host component is based upon either an untrusted operating system[1] or a trusted operating system[2] that does not support labeled security. The host component is intended to operate in a single information domain at a time. The host component is also intended to operate in accordance with appropriate periods processing policies that ensure a sanitized state is traversed between domain sessions. This profile allows the host component hardware and operating system to be part of the TOE, but does not allow them to be part of the TSF.

  A manual periods processing host capability is necessary because the network component will be unable to receive labeled information from the host component, and the host component will be unable to maintain the labels associated with the information received from the network component. Once information is within the scope of control of the host component, its protection becomes a function of operational policy that is not enforced by the TOE.

- **Management Component.** The management component provides all the capabilities to securely install, initialize, configure and operate the TOE and to manage TOE users. The management component may be implemented as a centralized dedicated capability, a centralized dynamically assignable capability, or as a de-centralized management capability. In the case of the dynamically assignable management capability, either manual, semi-automatic, or fully automatic processes would be required to move information from one management host to another. In the case of the de-centralized management capability, the issues of primary/backup, controlling management component, information replication and maintenance of consistent states would have to be addressed. Although this profile makes no assumptions regarding the implementation of this capability, this profile also does not address requirements specific to a de-centralized implementation.

[1] Win9x, majority of UNIX implementations, Linux, MacOS

[2] some Windows NT and UNIX implementations

- **User Component.** The user component provides the capabilities to enforce information flows to ensure that domain communication occurs in a manner that is consistent with the information flow policy that is in effect. The user component interfaces with the reader component and the management component in support of domain participation authentication, which includes the association of a specific information flow policy with the authenticated user.

  The user component interacts with other instances of the TOE to provide end-to-end domain communication. For this communication, both instances of the TOE must be authenticated as members of the same domain, and the two instances of the TOE negotiate to establish the cryptographic services that will be used for their communication session.

  The user component also interacts with the host component to enforce the periods processing requirements when switching from one domain to another.

- **Credential Input Component.** The credential input component provides the capability for communication between individuals and the TOE for authentication and establishment of participation in a domain. The credential input component may be an integral, non-separable physical component of the TOE, may be an external device interfaced directly with other components of the TOE or may be interfaced with other TOE components through an indirect interface. The actual form and function of the credential input component is determined by both the strong authentication technology employed and the implementation of that technology into the TOE (e.g., biometrics, hardware token, SmartCard).

  Should the vendor choose to satisfy any aspects of the security objectives in this profile with functional capabilities implemented through IT technology read by the credential input component, then that IT technology is considered part of the TSF. The Security Target must completely address this IT technology and demonstrate how it is incorporated into the TSF.

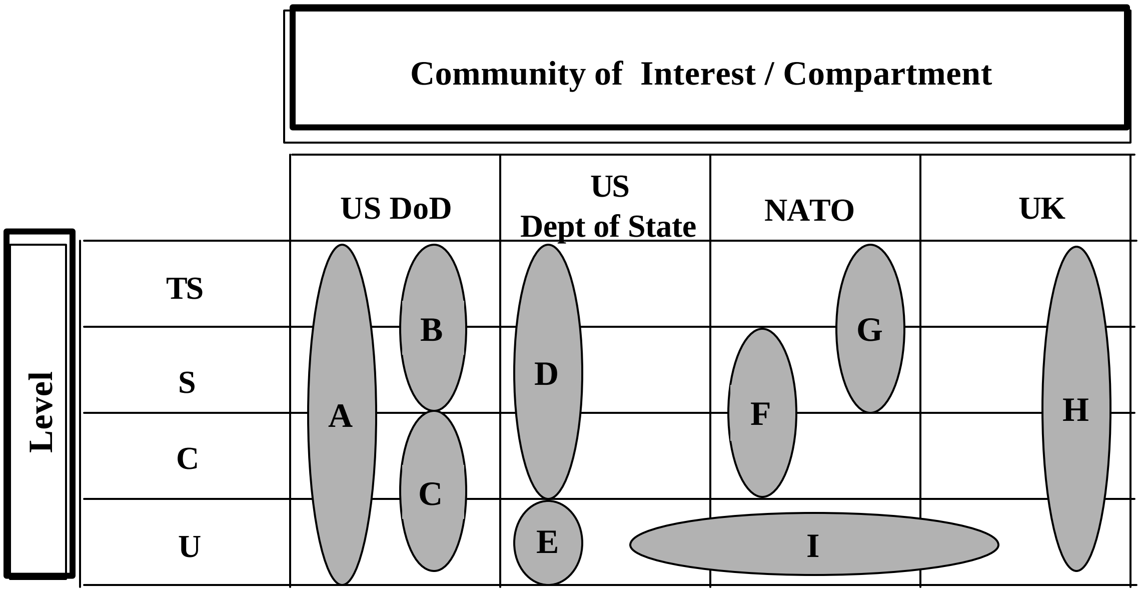
The TOE capabilities will be introduced and discussed in the context of information domains, domain participation authentication, domain isolation, management, periods processing, and key management. This discussion supports later illustration of the scope and boundaries of the TOE, anticipated TOE use cases to include the relationship between the TOE and its operational environment.

A separate discussion found in Appendix A addresses real-world scenarios and use-cases for employment of the TOE.

3.2 TOE Capabilities

3.2.1 Information Domain Concept

An information domain, referred to as a *domain* in this profile, is a logical concept. A domain is a unique information context defined by a set of attributes that characterize the information within the domain. As an example, Mandatory Access Control policy establishes a hierarchical relationship based upon information labels (e.g., Unclassified, Confidential, Secret, Top Secret) and non-comparable relationships based upon information labels and compartments (e.g., Secret/Nuclear, Confidential/Special Ops). In this information context, a domain may be defined in terms of discrete labels, discrete label and compartment combinations, ranges of labels, or ranges of labels and compartment combinations.



Definitions of Sample DOMAINS: A, B, C, …., I

The TOE ensures the isolation of domains through enforcement of a Domain Information Flow Policy (DIFP). The DIFP defines and enforces the rules through which the TOE allows or disallows information flows to occur between authenticated users.[3] DIFP enforcement rules are based upon/defined in terms of the following attributes:

- A unique domain identification

[3] Two users may be authenticated by their respective TOEs, but are not allowed to communicate because they are not participants in the same domain, or there may be other restrictions that prevent them from communicating., and such restrictions would be incorporated into an instance of the DIFP.

- A unique user/TOE pair identity
- A unique identification for information flows in a domain
- The type of information flow allowed (e.g., send, receive)
- Explicitly allowed or prohibited information flows
- Protected and unprotected information flows
- The cryptography service(s) employed to protect information

Organizational policies and operating procedures are used to establish the security context for the definition of domains, for the allowed and disallowed information flows in the domains, and for the correctness of these definitions. Relevant organizational policies must be translated into the DIFP. An instance of the DIFP that is enforced by the TOE is referred to as a *personality*. Both the TOE and the individual may have one or more personalities. The set of personalities associated with the TOE or with an individual is referred to as a *profile*.

The specific personality enforced by the TOE is determined by an authentication session that establishes participation in one domain for the combination of the TOE and an individual. This authentication session is referred to as *Domain Participation Authentication (DPA)*, and this authentication process must complete successfully before any information flow is allowed to occur.

The TOE enforces a personality without regard for the configuration of the host. The individual is responsible for ensuring that the host configuration is consistent with the personality enforced by the TOE.

3.2.2 Domain Participation Authentication Policy (DPAP)

The DPA capability of the TOE employs strong authentication mechanisms to authenticate a request for participation in a domain. Upon successful authentication for participation in a domain, the TOE applies the personality associated with that domain, and then allows communication to occur with other participants in the same domain. The TOE is capable of associating DPA credentials, domain identifiers and DIFP enforcement rules. Each domain identifier that requires isolation services is also associated with at least one encryption mechanism.

A DPA decision is based upon the following criteria:

- The domain(s) for which the *individual* is authorized participation, and
- The domain(s) for which the *TOE* is authorized participation.

The TOE/individual combination must become a participant in a domain in order to communicate with other TOEs in that domain. Independently, the TOE and the individual may each be *authorized* for participation in many domains. The combination of the TOE and the individual defines a subset of those combinations as *potential* participation domains. The DPA will authenticate the TOE/individual for *actual* participation in only one domain at a time.

Domain authentication credentials are required to support DPA. These credentials are required for both the individual and the host component of the TOE, and are provided, in part, through employment of hardware token technology. The TOE's credentials are uniquely associated with the TOE by an administrator during the TOE installation/initialization process. The DPA mechanism requires the individuals credentials and the TOE's credentials to determine the domain in which the TOE/individual combination shall be authenticated for participation.

Once a TOE/individual combination is authenticated and granted participation in a domain, the TOE is able to conduct steady-state security operations for the duration of that domain participation session. The TOE prevents simultaneous participation in any other domain while a domain participation session is active. Domain participation must be terminated before the establishment of participation in a new domain. The termination of a domain participation session results in the TOE, and therefore the individual, not participating in any domain. Domain participation may be terminated by the individual (i.e., the individual chooses to leave the domain or chooses to join some other domain) or by an administrator. Administrator termination includes the capability for *immediate revocation* of authorization to participate in a domain. In such cases, the current domain participation session is terminated and the individual and/or TOE are then prevented from future participation in that domain.

The TOE is capable of providing a human readable indication of the domain in which it is participating. This indication may take the form of an encoding (e.g., LED array w/octal readout), or may take the form of alphanumeric characters (e.g., readout on Credential Input Component).

The TOE provides a trusted path to the individual for the input of their DPA credentials. The trusted path is provided to the DPA mechanism through the credential input component of the TOE.[4]

3.2.3 Domain Isolation

The TOE ensures domain isolation through enforcement of the DIFP that defines the allowable information flows for a given domain. Enforcement of the DIFP is implemented through the application of cryptography services that are associated with each domain definition. These services provide for data confidentiality and integrity and require instances of the TOE[5] at the endpoints of each domain communication to provide the encrypt/decrypt capability of all

[4] There are implications to the trusted path requirement. If kept, the TOE may not rely on the host O/S to provide input of credentials to the TOE because there is no trusted path capability in the O/S **if** the O/S is untrusted. If the O/S is trusted, there **may** not be a trusted path capability. Furthermore, this profile makes the assumption that the host O/S is not part of the TSF – so, any security functionality provided by the host O/S is out of the scope of this profile – and is not evaluated. B2 required trusted path; if this product is meant to meet B2 functionality, the trusted path must remain. If this product is primarily meant to meet B2 assurance, then the trusted path requirement may be removed.

[5] The MDS PP defines the requirements for an instance of the TOE, to include the requirements for TOE-to-TOE interaction. Although two instances of the TOE are required for communication, the TOE is not a distributed pair of components. The TOE is multiply instantiated in an operational environment.

protected information flows.[6] For protected information flows, a trusted channel is established between the communicating TOEs. An information flow between the TOEs cannot occur until the trusted channel is established. The sending TOE negotiates with the receiving TOE and reach consensus on the specific means of communication. The sending/receiving TOEs process every packet of information that is transmitted between them. The sending/receiving TOEs also employ authentication and replay services to further protect domain communications.

3.2.4 TOE Management

The TOE provides management capabilities to install, configure and monitor the operation of instances of the TOE. These capabilities include the following:

- DPA Management
    - the creation, destruction, and maintenance of DPA credentials
    - the creation, maintenance and deletion of user accounts
    - the configuration of authentication processes
    - profile specification and association with individual users
- DIFP Management
    - the definition of DIFP instances
    - the maintenance of personalities and profiles
- Cryptographic service management
- Audit Management
    - the management of audit trail configuration, and event collection and review capabilities of management components
    - the management of the event recording configuration for user components
    - the management of notifications that signal potential DIFP or other defined policy violations.

3.3 TOE IT Environment Description

A dependency of the TOE upon security services provided by its IT environment require that the interface requirements between the TOE and the system or product which provides the services be defined.

The TOE is envisioned to interact with two such devices: the Electronic Key Management System (EKMS), and other instances of the TOE.

[6] The TOE supports a “no services” or in-the-clear communication mode whereby there are no cryptography services applied to the information flow.

3.3.1 EKMS Interoperability

The TOE interacts with the Electronic Key Management System that provides for the generation, distribution, and control of public key certificates and associated public keys intended for cryptography-enabled services. EKMS will provide suitable ordering, validation, generation, accounting, destruction, and compromise handling.[7]

3.3.2 Other TOE Instances

The TOE requires a separate instance of the TOE to be in place to serve as an endpoint for each protected communication path within a domain. The separate instance of the TOE meets all the security requirements defined and allocated to the TOE by this profile. There are no requirements unique to that separate instance. The separate instance of the TOE is addressed in this section only to reinforce the concept that the TOE depends upon that separate instance as a component in its IT environment. From the perspective of one instance of the TOE, the other instance is a trusted product with which it must communicate. All the requirements for the TOE, and for its communication with another instance of the TOE, are defined in the security functional requirements section.

[7] "Information Assurance Technical Framework," Release 2.0.1, September 1999, Issued by the National Security Agency, Solution Development and Deployment, Technical Directors

4 Security Environment

4.1 Assumptions

This section describes security aspects of the environment in which the TOE will be used or is intended to be used. This includes information about the physical, personnel, and connectivity aspects of the environment.

A conformant TOE can only provide effective security measures if it is installed and operated in a manner that is consistent with these assumptions. This profile contains assumptions in the following contexts:

- TOE Integration – the assumptions serve as needs levied on the non-IT environment of the TOE for the integration of the TOE with its non-IT and IT environment. With respect to the IT environment these assumptions only address the existence of capabilities that the IT environment must provide to support the TOE (e.g., The TOE obtains Directory Services from its IT environment). The requirements for the IT environment to *interface* with the TOE for the establishment of a trust relationship and to exchange information are not assumptions (e.g., the authentication requirements for establishment of a trust relationship with a Directory Server). Such requirements are defined in the section of this profile that discusses requirements for the IT environment of the TOE.
- TOE Usage – the assumptions serve to establish bounds on what is and what is not expected of the TOE in terms of its capabilities and appropriate or intended use.
- TOE Interaction with other IT – the assumptions serve to establish bounds on the relationship between the TOE and elements of its IT environment.

A.Host_Platform

The host platform does not use non-volatile storage capabilities (e.g., PROM, EEPROM, and Flash Memory) to store domain specific information.

The scope of this assumption is the hardware and firmware that is integral to the implementation of the host. The TSF forces the host to transition through an information-neutral state before establishing domain participation. This information-neutral state is limited in scope to volatile memory components of the host.

Persistent storage devices such as hard drives, zip drives and writeable CDs are not within the scope of this assumption (refer to A.No_MLS_Operation).

A.No_MLS_Operation

It is assumed that the host O/S of the TOE does not provide information flow control capabilities, and therefore, the TOE is not intended to operate as a multi-level security (MLS) system.

Without an information flow control capability (e.g., the ability to enforce a Mandatory Access Control policy), the host component O/S can not extend the domain isolation capabilities provided by the network component to its scope of control. In addition, the persistent storage devices (e.g., hard drives, zip drives, writeable CD drives) are also unable to provide domain isolation capability. The TOE Scope of Control (TSC) ends at the interface to the host component O/S (i.e., where the network component interfaces with the host component O/S).

The operational environment has complete responsibility for ensuring the isolation of domain information stored on the host. The environment must implement appropriate policies and procedures to ensure that domain isolation principles are enforced on the host component.

Two significant issues arise from this assumption:

1. The host component O/S may be an evaluated trusted or unevaluated untrusted product. In either case, the O/S does not support information flow control policies. An MDS that incorporates an MLS trusted operating system would be specified in a different profile.
2. Since the information flow control policy to be enforced by the TOE is defined by the organization that employs the TOE, it is possible to define a domain to include multiple levels (i.e., System high – SECRET.) In such a case, the TSF would label all information flows in the domain as SECRET. The host O/S would be unable to associate a label with the information, therefore, all persistent storage would have to be treated as SECRET.

A.Host_Periods_Processing

Prior to joining a domain, periods processing of the host component is performed manually by the user of the TOE.

Under normal operating conditions, periods processing is initiated by the human user to ensure sanitization of volatile host memory hardware.

A.Storage_Media

Writeable storage media is not used in a manner that allows domain information to cross domain boundaries.

All storage media (floppy disks, removable harddrives, tapes, etc) is properly labeled and handled in a manner that prevents unauthorized access to the stored data.

A.TOE_Transparency

The TOE is transparent to application level processes. The TOE does not interface with these processes and does not read, change the contents of, or interpret the information (i.e., the payload) transmitted by application level processes.

The TOE provides a virtual channel for information to flow between application level processes. Since the TOE restricts information flows to the domain in which the TOE is participating, the TOE does not require access to the contents of the information transmitted in order to provide and enforce secure information flows. Therefore, there is no need for application level processes to be cognizant of the TOE.

A.Network

The characteristics of the network(s) to which the TOE interfaces (i.e., LAN, WAN, Internet Connectivity, local-dedicated) do not restrict TOE use.

Network topology and geographical bounds are not an issue for the operational use of the TOE. If such constraints do exist, any derived PP/ST must ensure that this assumption is appropriately re-worded, removed from this profile, or augmented with additional assumptions that capture any constraints or restrictions on TOE use.

A.Physical_Protection

The environment is capable of physically protecting the TOE by signaling the occurrence of fire, flood, power loss, and environmental control failures that might adversely affect TOE operations.

The environment must provide appropriate means to ensure that notifications of such events occur with sufficient lead-time to ensure that the TOE may be shutdown before entering a non-secure state.

A.Crypto_Support

Cryptographic support infrastructure will be provided by procedures and mechanisms external to the TOE. Examples: user registration, key issuance, directory services, and assignment of privileges.

4.3 Threats

This section specifies the threats that exist in the security environment of the TOE, and that must be countered by some combination of the TOE and its security environment.

T.Tamper

An individual replaces or alters TOE components such that the DIFP is no longer enforced. Unauthorized access to domain information or resources then occurs by that individual or by other individuals regardless of whether or not they have been authenticated to domains.

- This statement does not apply to Type-1 cryptographic devices interfaced to the TSF. Type-1 devices require anti-tamper as part of their certification.

T.Audit

Accountability for security-relevant activities performed by the TOE is impossible to ascertain because the TOE does not:

- record events pertaining to the actions of TOE users
- record events pertaining to TSF actions (authentication, audit, startup/shutdown, information flows)
- associate the individual, the TOE, or the individual/TOE pair with recorded events,
- protect audit records from loss due to audit trail failure or due to excessive volume of records (i.e., saturation of audit storage device)

T.Covert_Channel

An individual with access to the TOE transmits information in a manner that is inconsistent with information flow policy via the use of covert channels.

T.Admin

The administrator performs actions that result in unauthorized access to domain information or resources.

An administrator could intentionally or unintentionally perform or fail to perform functions, (e.g. system configuration, perform system integrity test) that directly compromise security objectives or change security policies enforced by the TSF.

T.Admin_Role

An individual obtains authorizations reserved for authenticated administrators and performs actions that violate policy.

An individual may obtain privilege to perform functions that should be restricted to admin personnel. The TOE must have appropriate functions to manage the TOE securely, and must have necessary checks to restrict users that are able to use those privileges.

T.Implementation

The TOE is not implemented in accordance with design specifications or contains flaws that prevent the TOE from operating securely**.**

The TOE is composed on hardware, software, and firmware. Each offers potential for incorrect implementation. Flawed code and back doors are examples of sources of potential failure of one or more system components, thus resulting in loss of system-critical security functionality.

T.Information_Flow

An individual with access to the network providing connectivity for TOE instances is able to gain access to information flows, or is able to modify, substitute, or replace information flows.

An individual may capture domain information for cryptanalysis and the subsequent unauthorized use of the deciphered information; may capture information flows and alter them by modifying flow contents, or may make partial or complete substitution of the information flow; or may interject information flows in an effort to flood the destination TOE, to replay previous information flows, or to masquerade as a legitimate TOE.

The scope of this threat is not the ability to recognize specific changes to the contents of an inserted or substituted information flow, it is only that an information flow has been substituted or interjected.

T.Unauthorized_TOE_Access

An individual bypasses or defeats TOE authentication mechanisms and obtains unauthorized use of domain information and resources.

Defeating the authentication mechanism (e.g., bypassing, subverting) may occur through attacks such as masquerading or brute force. This threat parallels the OSPs that address authentication mechanisms and authentication credentials.

T.Domain_Isolation

An individual with authorized access to the TOE is able to gain unauthorized access to domain information due to the inability of the TOE to isolate domain information.

An individual with authorized access is a legitimately authenticated individual. The scope of this threat is the inability of the TOE to properly isolate domains once the TOE/individual is authenticated. Refer to the threat T.Unauthorized_TOE_Access that addresses the threat of an unauthorized individual being able to obtain access to the TOE.

T.Domain_Information_Reuse

An individual authenticated for participation in a domain gains unauthorized access to previous domain information. This is possible because residual information from the previous domain participation session remains available upon the establishment of the new domain participation session.

The unauthorized access to domain information may occur because the TOE transmits residual domain information without the user knowing that the transmission occurs.

T.Bridge

An individual authenticated for participation in one domain simultaneously authenticates for participation in a different domain (from the same TOE) and contaminates the information in either or both domains.

A TOE that bridges multiple domains allows simultaneous access to those domains and other users participating in those domains may send information to the TOE that is acting as a bridge without the user knowing what is going on.

T.TOE_Failure

TOE failure results in either

- the compromise of domain information such that the DIFP is not enforced,
- an authorized user being denied access to domain information and resources.

T.TSF_Integrity

Corruption of the TSF results in the inability of the TSF to enforce DIFP and the inability of the TSF to continue secure operations.

The definition of TSF includes audit, authentication, access controls, DIFP enforcement functions.

This threat address changes to the TSF by replacement or modification. The TSF must be able to protect itself to ensure its integrity.

T.TSF_Bypassability

The TSF is bypassed allowing unmediated access (i.e., unauthorized access) to domain information.

This threat addresses the ability for untrusted processes or individuals to circumvent the TSF to obtain unauthorized access to protected information and resources.   The TSF is unable to enforce the DIFP if TSF bypass attempts succeed.

4.3 Organizational Security Policies (OSPs)

This section specifies the OSPs that must be enforced by some combination of the TOE and its security environment.

P.Authentication_Credentials

Credentials used to authenticate the access to IT systems shall be provided to authorized individuals and shall be made available to the systems responsible for enforcing security policy.

> This policy requires a process to define, create, and distribute DPA credentials for authentication to those individuals that use the services provided by the TOE. The TOE supports this policy through its ability to create and manage DPA credentials and its ability to distribute DPA credentials to instances of the TOE.

P.Strong_Authentication

All users shall be authenticated by two-factor strong authentication mechanisms prior to being granted access to systems and the information and resources managed by those systems.

> This policy requires authentication processes to be explicitly selected and employed. The TOE supports this policy through the DPA mechanism based on hardware token technology. Additionally, the TOE supports this policy by requiring both the TOE and the individual to be authenticated as a coupled pair before allowing participation in a domain and before allowing any information flows between the TOE and other domain participants.

P.Credential_Protection

Authentication credentials shall be protected to prevent unauthorized access, modification or destruction.

> This policy requires that all credentials be adequately protected by the individuals and IT entities that make use of those credentials. The TOE supports this policy by restricting access to DPA credentials, by protecting the credentials as they are transmitted over the network during the domain authentication process, and through the trusted path between the credential reader and other TOE components.

P.Domain_Information_Flow_Policy

A domain information flow policy shall be enforced to ensure that only the following information flows occur:

- Information flows between two TOEs authenticated to the same domain
- Information flows between the TOE and a non-TOE protected host. The TOE shall be authenticated and restricted to only send/receive information flows, in-the-clear, with non-TOE hosts.

P.Training

All users shall be trained to understand applicable system-use policies, the proper use of systems and the vulnerabilities inherent to those systems.

> This policy ensures that all users are properly instructed on policies and procedures for using the system, as well as, being able to acknowledge all threats and vulnerabilities that may impact system processing. TOE documentation supports this policy.

P.Trusted_User

All users shall abide by designated policies and the conduct stated by those policies.

> In this context, users includes both users of systems that interface with the TOE, and the administrators of systems that interface with the TOE in addition to the administrators of the TOE. This policy covers use and adherence to policies, procedures, system, admin, and user documentation, associated with the TOE and all systems that interface with the TOE.

P.Policy_Violation_Notification

Administrative personnel shall be notified of discrete events that may indicate a violation of enforced policy.

P.Cryptography

Cryptographic services that are used to ensure information confidentiality, privacy or integrity shall meet the criteria of the appropriate robustness (strength of mechanism and assurance) based on the value of information to be protected and the threat environment.

5 Security Objectives

5.1 TOE Security Objectives

This sections contains the security objectives to address the assumptions and counter the threats stated within this PP.

O.Credentials

The TSF shall be capable of managing credentials that are used to support Domain Participation Authentication and to authenticate TOE administrators.

> Manage – Create, delete, modify, store, retrieve, and validate
>
> The requirement to distribute credentials must be addressed IF it is inherent to the implementation of the administration functions. This will have to be addressed in the ST and we have to put the pointer in the relevant assignment and selection operations.

O.Domain_Participation_Authentication

The TSF shall implement at least one two-factor strong authentication mechanism based upon token technology and cryptographic services in support of domain participation. The TOE and the individual must be authenticated as a coupled pair before granting participation in a domain and before allowing any information flows between the TOE and other domain participants.

O.Domain_Indication

The TSF shall provide visible indication of active domain participation.

> The indication is managed as TSF data.
>
> The indication may be an encoding of the domain identifier or an alpha-numeric readout.
>
> Since the host O/S is not part of the TSF, the indication can not be provided to the user through the host O/S, its user interface, or through other host O/S controlled peripheral devices.

O.Audit

The TSF shall be able to audit the events listed below. The TSF shall be able to associate events with the individual and/or TOE that caused the event to occur. The TSF shall include details relevant to each event and at a minimum, shall include the date and time that the event occurred.

- DPA session events (initiation/authentication, termination, etc)
- Domain information flow events
- DIFP policy violations
- Administrative events

O.Audit_Management

The TSF shall provide the functions to support the administrator's management and review of audit events.

O.Audit_Protection

The TSF shall protect the audit trail from event loss due to audit trail failure or saturation of the audit storage device.

O.Immediate_Violation_Notification

The TSF shall be able to provide immediate notification to administrator personnel for the following discrete events that indicate a violation of enforced policy:

O.Cryptography

The TSF shall interface with certified cryptographic support mechanisms that provide cryptography services.

O.Single_Domain

The TSF shall prevent an individual/TOE pair from simultaneous participation in more than one domain.

O.Cryptographic_Services

The TSF shall be capable of associating and employing one or more cryptographic service with each unique domain definition.

Cryptographic services, to include hashing, digital signatures.

O.Information_Reuse

The user, network, credential input, and management component TSFs shall ensure that residual information associated with a terminated domain session is not available upon establishment of a new domain session.

O.Management

The TSF shall provide functions necessary to install, operate, and maintain TOE instances. The TSF shall implement controls to ensure that these functions may be invoked only by those individuals that have been authenticated as authorized administrators of the TOE.

The TSF shall provide, at a minimum: Audit, Authentication, DIFP definition…

An authorized user may obtain privilege to perform functions that should be restricted to admin personnel. The TOE must have appropriate functions to manage the TOE securely, and must have necessary checks to restrict users that are able to use those privileges.

O.Trusted_Communication

The TSF shall establish a trusted channel between itself and another TOE instance for each TOE-to-TOE domain information flow. The trusted channel shall be established via a TOE-to-TOE authentication session that is based upon cryptographic services.

O.Policy_Definition

The TSF shall provide a capability for defining personalities that are associated independently with each individual and with each instance of the TOE. The TSF shall be capable of grouping personalities into profiles.

O.Policy_Enforcement

The TSF shall enforce the domain information flow policy defined by the personality that the individual/TOE pair is authenticated to use.

The TSF shall explicitly prohibit:

- information flows between TOEs authenticated to different domains

The TSF shall explicitly allow:

- in-the-clear communication flows between:
    1. the TOE and any host that is not protected by an instance of the TOE,
    2. the TOE and other instances of the TOE

  For explicitly allowed in-the-clear communication, the TOE shall be authenticated and then restricted to only send/receive information flows with non-TOE hosts and with other TOE instances that have also been authenticated and restricted for explicitly in-the-clear communication.

If none of the previous conditions are met, the TSF shall mediate information flows based upon the following attributes:

- domain identification
- security levels and categories (e.g. levels, categories, compartments)
- allowed/disallowed information flows within the domain
- the cryptographic services and algorithms used to implement information flows in the domain
- the cryptographic services and algorithms that are used to implement TOE-to-TOE trust relationships

O.EKMS

The TSF shall implement EKMS-defined requirements for secure key generation, distribution, and trust establishment interactions with the EKMS.

O.TSF_Implementation

The TSF shall be implemented in accordance with design specifications and shall be tested to verify correct implementation.

We need EAL4 justification to go here…

O.TSF_Protection

The TSF shall capable of protecting itself (security functions and data) from unauthorized access and modification.

TSF data includes DPA credentials, audit data, etc….

This objective covers the aspects of TSF self-protection (domain separation), privileged access to TSF functions, and privileged access to TSF data.

O.TSF_Integrity

The TSF shall be capable of demonstrating the integrity of its binary image [fill-in: as provided on storage media, when in an operational state] as well as the correct operation of the binary image and any hardware/firmware during [fill-in: during installation, power up/shutdown, initialization, on-demand].

This is tied to O.Fail_Secure.

O.TSF_Non_Bypassability

The TSF shall be implemented to ensure that

- the TSF is always invoked for each and every TSF-mediated action
- no security-relevant action successfully completes unless the TSF explicitly allows it.

O.Fail_Secure

The TSF shall enter a secure state such that information flows are disabled upon detection of any condition that prevents it from continuing to operate securely.

5.2 Non-IT Environment Security Objectives

OE.Host_Platform

The individuals responsible for the TOE must ensure that the host platform non-volatile storage capabilities (e.g., PROM, EEPROM, and Flash Memory) are not modified such that they are able to violate the DIFP (i.e., no domain information is stored in these memory devices and later accessed when domain membership changes).

This objective applies only to the hardware and firmware that is integral to the implementation of the host.

OE.Host_Operation

The individuals responsible for the TOE must ensure that the TOE is not used to support multi-level security (MLS) operations.

OE.Policy_Def_&_Translation

The organization responsible for managing the TOE must ensure that

- domains are properly defined (e.g., define red, blue, green)
- domain information flow policies are correctly defined in accordance with the domain definitions (e.g, define how red communicates with red, blue with blue, green with green)
- domain information flow policies are correctly translated into the DIFP. (e.g., translate the two preceding bullets into something the TOE understands, implements, and enforces)

Organizational security policies for allowed and disallowed domain information flows form the basis to establish the security context for the definition of domains, for the allowed and disallowed information flows in the domains, and for the correctness of these definitions. All relevant organizational policies must be translated into the DIFP.

OE.Host_Periods_Processing

The individuals responsible for the TOE must ensure that the user of the TOE performs periods processing of the host component prior to joining a domain.

OE.Storage_Media

The individuals responsible for the TOE must ensure that writeable storage media is not used in a manner that allows domain information to cross domain boundaries.

OE.TOE_Transparency

The developers of the TOE must ensure that the TSF is transparent to application level processes, and does not require any interaction with application processes to meet TOE objectives.

OE.Network

The developers of the TOE must ensure that the TSF is not dependent upon or affected by the characteristics of the network(s) to which the TOE is interfaced to meet its objectives.

OE.Physical_Protection

The individuals responsible for the TOE must ensure that the environment is capable of physically protecting the TOE by signaling the occurrence of fire, flood, power loss, and environmental control failures that might adversely affect TOE operations.

OE.Tamper_Protection

The individuals responsible for the TOE must provide tamper detection seals that allow authorized personnel to detect unauthorized access to physical TOE components (e.g., host workstation).

OE.Authentication_Credentials

The individuals responsible for the TOE must ensure that credentials used to support DPA are properly defined, created, and distributed.

This applies to the TOE and to users of the TOE.

OE.Credential_Protection

The individuals with responsibility for the use and handling of authentication credentials must ensure that they are protected to prevent unauthorized access.

OE.Training

The individuals responsible for managing and operating the TOE must ensure that all individual users of the TOE are trained to understand applicable system-use policies, the proper use of the TOE, and the vulnerabilities inherent to the operation of the TOE.

This policy ensures that all users are properly instructed on policies and procedures for using the system, as well as, being able to acknowledge all threats and vulnerabilities that may impact system processing. TOE documentation supports this policy.

OE.User_Trust

The individuals responsible for managing and operating the TOE must ensure that individual users of the TOE understand their responsibility to comply with all relevant policies.

In this context, ‘users’ includes both users of systems that interface with the TOE, and the administrators of systems that interface with the TOE in addition to the administrators of the TOE. This policy covers use and adherence to policies, procedures, system, admin, and user documentation, associated with the TOE and all systems that interface with the TOE.

OE.TOE_Failure

The individuals responsible for the TOE must ensure that failure of the TOE does not result in an unacceptable period of denial of TOE services.

The TOE has no fault-tolerant capabilities. The operators of the TOE must be prepared to replace the TOE should it fail, and to do so within a reasonable amount of time (i.e., perhaps as defined by performance policies, contracts, guidelines, etc).

5.3 IT Environment Security Objectives

OIE.EKMS

The EKMS shall define the requirements for secure interaction with the TSF. These interface requirements shall address:

- Establishment of trust
- Interactions in support of key generation and distribution

6 TOE Security Requirements

6.1 TOE Functional Requirements

815 The functional security requirements for this PP consist of the following components from Part 2, summarized in the following table.

Functional Class	Functional Components	
Security Audit	FAU ARP.1	Security Alarms
	FAU GEN.1	Audit Data Generation
	FAU GEN.2	User Identity Association
	FAU SAA.1	Security Audit Analysis
	FAU SAR.1	Audit Review
	FAU SAR.3	Selectable Audit Review
	FAU SEL.1	Selective Audit
Cryptographic Support	FCS CKM.1	Cryptographic Key Generation
	FCS CKM.4	Cryptographic Key Destruction
	FCS COP.1	Cryptographic Operation
User Data Protection	FDP ACC.1	Subset Access Control
	FDP ACF.1	Security Attribute Based Access Control
	FDP IFC.1	Subset Information Flow Control
	FDP IFF.1	Simple Security Attributes
	FDP RIP.1	Subset Residual Information Protection
Identification and	FIA ATD.1	User Attribute Definition
	FIA UAU.2	User Authentication Before Any Action
	FIA UAU.5	Multiple Authentication Mechanisms
	FIA UID.1	Timing of Identification
	FIA UID.2	User Identification Before Any Action
Security Management	FMT MSA.1	Management of Security Attributes
	FMT MSA.2	Secure Security Attributes
	FMT MSA.3	Static Attribute Initialisation
	FMT MTD.1	Management of TSF data
	FMT REV.1	Revocation
	FMT SMR.1	Security Roles
Protection of the TOE	FPT ITC.1	Inter TSF Confidentiality During Transmission

Functional Class	Functional Components	
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.2	SFP Domain Separation
	FPT_STM.1	Reliable Time Stamps
	FPT_TST.1	TSF Testing
TOE Access	FTA_MSC.1	Limitation on Scope of Selectable Attributes

Table 6-1. Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1)

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection: *minimum, basic, detailed, not specifie*d] level of audit; and

c) [assignment: *other specifically defined auditable event*s].$^{\text{FAU\_GEN.1.1}}$

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant informatio*n]$^{\text{FAU\_GEN.1.2}}$

6.1.1.2 User identity association (FAU_GEN.2)

The TSF shall be able to associate each auditable event with the identity of the user that caused the event.$^{\text{FAU\_GEN.2.1}}$

6.1.1.3 Audit review (FAU_SAR.1)

The TSF shall provide [assignment: *authorised user*s] with the capability to read [assignment: *list of audit informatio*n] from the audit records.$^{\text{FAU\_SAR.1.1}}$

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.$^{\text{FAU\_SAR.1.2}}$

6.1.1.4 Restricted audit review (FAU_SAR.2)

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. [FAU_SAR.2.1]

6.1.1.5 Selectable audit review (FAU_SAR.3)

The TSF shall provide the ability to perform [selection: *searches, sorting, orderin*g] of audit data based on [assignment: *criteria with logical relation*s].[FAU_SAR.3.1]

6.1.1.6 Selective audit (FAU_SEL.1)

The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [selection: *object identity, user identity, subject identity, host identity, event typ*e]

b) [assignment: *list of additional attributes that audit selectivity is based upo*n].[FAU_SEL.1.1]

6.1.1.7 Potential violation analysis (FAU_SAA.1)

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.[FAU_SAA.1.1]

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment: *subset of defined auditable event*s] known to indicate a potential security violation;

b) [assignment: *any other rule*s]. [FAU_SAA.1.2]

6.1.1.8 Security alarms (FAU_ARP.1)

The TSF shall take [assignment: *list of the least disruptive action*s] upon detection of a potential security violation. [FAU_ARP.1.1]

6.1.2 Cryptographic Services (FCS)

6.1.2.1 Cryptographic operation (FCS_COP.1)

6.1.2.2 The TSF shall perform [assignment: *list of cryptographic operation*s] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorith*m] and cryptographic key sizes [assignment: *cryptographic key size*s] that meet the following: [assignment: *list of standard*s] FCS_COP.1.1

6.1.3 User Data Protection (FDP)

6.1.3.1 Subset access control (FDP_ACC.1)

The TSF shall enforce the [assignment: *access control SF*P] on [assignment: *list of subject*s, *objects, and operations among subjects and objects covered by the SF*P]. FDP_ACC.1.1

6.1.3.2 Subset access control (FDP_ACF.1)

The TSF shall enforce the [assignment: *access control SF*P] to objects based on [assignment: *security attribute*s, *named groups of security attribute*s]. FDP_ACF.1.1

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled object*s]. FDP_ACF.1.2

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to object*s]. FDP_ACF.1.3

The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to object*s]. FDP_ACF.1.4

6.1.3.3 Subset information flow control (FDP_IFC.1)

The TSF shall enforce the [assignment: *information flow control SF*P] on [assignment: *list of subject*s, *information, and operations that cause controlled information to flow to and from controlled subjects covered by the SF*P]. FDP_IFC.1.1

6.1.3.4 Simple security attributes (FDP_IFF.1)

The TSF shall enforce the [assignment: *information flow control SF*P] based on the following types of subject and information security attributes: [assignment: *the minimum number and type of security attribute*s].$^{\text{FDP\_IFF.1.1}}$

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attribute*s].$^{\text{FDP\_IFF.1.2}}$

The TSF shall enforce the [assignment: *additional information flow control SFP rule*s].$^{\text{FDP\_IFF.1.3}}$

The TSF shall provide the following [assignment: *list of additional SFP capabilitie*s]. $^{\text{FDP\_IFF.1.4}}$

The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flow*s]. $^{\text{FDP\_IFF.1.5}}$

The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flow*s]. $^{\text{FDP\_IFF.1.6}}$

6.1.3.5 Subset residual information protection (FDP_RIP.1)

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource t*o, *deallocation of the resource fro*m] the following objects: [assignment: *list of object*s].$^{\text{FDP\_RIP.1.1}}$

6.1.4 Identification & Authentication (FIA)

6.1.4.1 User attribute definition (FIA_ATD.1)

The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attribute*s]$^{\text{FIA\_ATD.1.1}}$

6.1.4.2 User authentication before any action (FIA_UAU.2)

The TSF shall require each user to be successfully authenticated before allowing **any other TSF-mediated actions** on behalf of that user. $^{\text{FIA\_UAU.2.1}}$

6.1.4.3 Multiple authentication mechanisms (FIA_UAU.5)

The TSF shall provide [assignment: *list of multiple authentication mechanism*s] to support user authentication.$^{\text{FIA\_UAU.5.1}}$

The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide authenticatio*n]. $^{\text{FIA\_UAU.5.2}}$

6.1.4.4 User identification before any action (FIA_UID.2)

The TSF shall require each user to identify itself before allowing **any other TSF-mediated actions** on behalf of that user.$^{\text{FIA\_UID.2.1}}$

6.1.5 Security Management (FMT)

6.1.5.1 Management of security functions behaviour (FMT_MOF.1)

The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour o*f] the functions [assignment: *list of function*s] to [assignment: *the authorised identified role*s].$^{\text{FMT\_MOF.1.1}}$

6.1.5.2 Management of security attributes (FMT_MSA.1)

The TSF shall enforce the [assignment: *access control SFP, information flow control SF*P] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operation*s]] the security attributes [assignment: *list of security attribute*s] to [assignment: *the authorised identified role*s].$^{\text{FMT\_MSA.1.1}}$

6.1.5.3 Secure security attributes (FMT_MSA.2)

The TSF shall ensure that only secure values are accepted for security attributes. $^{\text{FMT\_MSA.2.1}}$

6.1.5.4 Management of TSF Data (FMT_MTD.1)

The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clea*r, [assignment: *other operation*s]] the [assignment: *list of TSF dat*a] to [assignment: *the authorised identified role*s].$^{\text{FMT\_MTD.1.1}}$

6.1.5.5 Revocation (FMT_REV.1)

The TSF shall restrict the ability to revoke security attributes associated with the [selection: *users, subjects, objects, other additional resource*s] within the TSC to [assignment: *the authorised identified role*s].$^{\text{FMT\_REV.1.1}}$

The TSF shall enforce the rules [assignment: *specification of revocation rule*s]. $^{\text{FMT\_REV.1.2}}$

6.1.5.6 Security roles (FMT_SMR.1)

The TSF shall maintain the roles [assignment: *the authorised identified role*s].$^{\text{FMT\_SMR.1.1}}$

The TSF shall be able to associate users with roles.$^{\text{FMT\_SMR.1.2}}$

6.1.6 TOE Access (FTA)

6.1.6.1 Basic limitation on multiple concurrent sessions (FTA_MCS.1)

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.$^{\text{FTA\_MCS.1.1}}$

The TSF shall enforce, by default, a limit of [assignment: *default numbe*r] sessions per user.$^{\text{FTA\_MCS.1.2}}$

6.1.7 Protection of the TOE Security Functions (FPT)

6.1.7.1 Abstract machine testing (FPT_AMT.1)

The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of an authorised user, other condition*s] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.$^{\text{FPT\_AMT.1.1}}$

6.1.7.2 Failure with preservation of secure state (FPT_FLS.1)

The TSF shall preserve a secure state when the following types of failures occur: *[assignment: list of failures in the TSF]*.$^{\text{FPT\_FLS.1.1}}$

6.1.7.3 Non-bypassability of the TSP (FPT_RVM.1)

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.FPT_RVM.1.1

6.1.7.4 SFP domain separation (FPT_SEP.2)

The **unisolated portion of the** TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.FPT_SEP.2.1

The TSF shall enforce separation between the security domains of subjects in the TSC.FPT_SEP.2.2

The TSF shall maintain the part of the TSF related to [assignment: *list of access control and/or information flow control SFP*s] in a security domain for their own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to those SFPs.FPT_SEP.2.3

6.1.7.5 Reliable time stamps (FPT_STM.1)

The TSF shall be able to provide reliable time stamps for its own use.FPT_STM.1.1

6.1.7.6 TSF testing (FPT_TST.1)

The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self test should occu*r] to demonstrate the correct operation of the TSF.FPT_TST.1.1

The TSF shall provide authorised users with the capability to verify the integrity of TSF data.FPT_TST.1.2

The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.FPT_TST.1.3

6.1.8 Trust Path/Channel (FTP)

6.1.8.1 Inter-TSF trusted channel (FTP_ITC.1)

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.[FTP_ITC.1.1]

The TSF shall permit [selection: *the TSF, the remote trusted IT produc*t] to initiate communication via the trusted channel.[FTP_ITC.1.2]

The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is require*d].[FTP_ITC.1.3]

6.2 Assurance Requirements

The assurance requirements levied on the developer consist of EAL 4 augmented and are summarized in Table 6-2.

Table 6-2. Assurance Requirements

Assurance Class	Assurance Components
ACM	ACM_AUT.1, ACM_CAP.3, ACM_CAP.4, ACM_SCP.2
ADO	ADO_DEL.2, ADO_IGS.1
ADV	ADV_FSP.1, ADV_FSP.2 ADV_HLD.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1, ALC_LCD.1,ALC_TAT.1
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_MSU.2, AVA_SOF.1 AVA_VLA.2

Table 6-2. Assurance Requirements (cont.)

6.2.1 Configuration management (ACM)

6.2.1.1 CM automation (ACM_AUT.1)

The developer shall use a CM system.[ACM_AUT.2.1D]

The developer shall provide a CM plan.[ACM_AUT.2.2D]

The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation, and to all other configuration items.[ACM_AUT.2.1C]

The CM system shall provide an automated means to support the generation of the TOE.[ACM_AUT.2.2C]

The CM plan shall describe the automated tools used in the CM system.[ACM_AUT.2.3C]

The CM plan shall describe how the automated tools are used in the CM system.[ACM_AUT.2.4C]

The CM system shall provide an automated means to ascertain the changes between the TOE and its preceding version.[ACM_AUT.2.5C]

The CM system shall provide an automated means to identify all other configuration items that are affected by the modification of a given configuration item.[ACM_AUT.2.6C]

6.2.1.2 Authorisation controls (ACM_CAP.3)

The developer shall provide a reference for the TOE.[ACM_CAP.3.1D]

The developer shall use a CM system.[ACM_CAP.3.2D]

The developer shall provide CM documentation.[ACM_CAP.3.3D]

The reference for the TOE shall be unique to each version of the TOE.[ACM_CAP.3.1C]

The TOE shall be labelled with its reference.[ACM_CAP.3.2C]

The CM documentation shall include a configuration list and a CM plan.[ACM_CAP.3.3C]

The configuration list shall describe the configuration items that comprise the TOE.[ACM_CAP.3.4C]

The CM documentation shall describe the method used to uniquely identify the configuration items.[ACM_CAP.3.5C]

The CM system shall uniquely identify all configuration items.[ACM_CAP.3.6C]

The CM plan shall describe how the CM system is used.[ACM_CAP.3.7C]

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.[ACM_CAP.3.8C]

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.[ACM_CAP.3.9C]

The CM system shall provide measures such that only authorised changes are made to the configuration items.[ACM_CAP.3.10C]

6.2.1.3 Generation support and acceptance procedures (ACM_CAP.4)

The developer shall provide a reference for the TOE.[ACM_CAP.4.1D]

The developer shall use a CM system.[ACM_CAP.4.2D]

The developer shall provide CM documentation.[ACM_CAP.4.3D]

The reference for the TOE shall be unique to each version of the TOE.[ACM_CAP.4.1C]

The TOE shall be labelled with its reference.[ACM_CAP.4.2C]

The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.[ACM_CAP.4.3C]

The configuration list shall describe the configuration items that comprise the TOE.[ACM_CAP.4.4C]

The CM documentation shall describe the method used to uniquely identify the configuration items.[ACM_CAP.4.5C]

The CM system shall uniquely identify all configuration items.[ACM_CAP.4.6C]

The CM plan shall describe how the CM system is used.[ACM_CAP.4.7C]

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.[ACM_CAP.4.8C]

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.[ACM_CAP.4.9C]

The CM system shall provide measures such that only authorised changes are made to the configuration items.[ACM_CAP.4.10C]

The CM system shall support the generation of the TOE.[ACM_CAP.4.11C]

The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.[ACM_CAP.4.12C]

6.2.1.4 Problem tracking CM coverage

The developer shall provide CM documentation.[ACM_SCP.2.1D]

The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.[ACM_SCP.2.1C]

The CM documentation shall describe how configuration items are tracked by the CM system.[ACM_SCP.2.2C]

6.2.2 Delivery and operation (ADO)

6.2.2.1 Deletion of modification (ADO_DEL.2)

The developer shall document procedures for delivery of the TOE or parts of it to the user.[ADO_DEL.2.1D]

The developer shall use the delivery procedures.[ADO_DEL.2.2D]

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.[ADO_DEL.2.1C]

The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.[ADO_DEL.2.2C]

The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.[ADO_DEL.2.3C]

6.2.2.2 Installation, generation, and start-up (ADO_IGS.1)

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.[ADO_IGS.1.1D]

The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.[ADO_IGS.1.1C]

6.2.3 Development (ADV)

6.2.3.1 Informal functional specification

The developer shall provide a functional specification.[ADV_FSP.1.1D]

The functional specification shall describe the TSF and its external interfaces using an informal style.[ADV_FSP.1.1C]

The functional specification shall be internally consistent.[ADV_FSP.1.2C]

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.[ADV_FSP.1.3C]

The functional specification shall completely represent the TSF.[ADV_FSP.1.4C]

6.2.3.2 Fully defined external interfaces

The developer shall provide a functional specification.[ADV_FSP.2.1D]

The functional specification shall describe the TSF and its external interfaces using an informal style.[ADV_FSP.2.1C]

The functional specification shall be internally consistent.[ADV_FSP.2.2C]

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.[ADV_FSP.2.3C]

The functional specification shall completely represent the TSF.[ADV_FSP.2.4C]

The functional specification shall include rationale that the TSF is completely represented.[ADV_FSP.2.5C]

6.2.3.3 Security enforcing high-level design (ADV_HLD.2)

The developer shall provide the high-level design of the TSF.[ADV_HLD.2.1D]

The presentation of the high-level design shall be informal.[ADV_HLD.2.1C]

The high-level design shall be internally consistent.[ADV_HLD.2.2C]

The high-level design shall describe the structure of the TSF in terms of subsystems.[ADV_HLD.2.3C]

The high-level design shall describe the security functionality provided by each subsystem of the TSF.[ADV_HLD.2.4C]

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.[ADV_HLD.2.5C]

The high-level design shall identify all interfaces to the subsystems of the TSF.[ADV_HLD.2.6C]

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.[ADV_HLD.2.7C]

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.[ADV_HLD.2.8C]

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.[ADV_HLD.2.9C]

6.2.3.4 Subset of the implementation of the TSF (ADV_IMP.1)

The developer shall provide the implementation representation for a selected subset of the TSF.[ADV_IMP.1.1D]

The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.[ADV_IMP.1.1C]

The implementation representation shall be internally consistent.[ADV_IMP.1.2C]

6.2.3.5 Descriptive low-level design (ADV_LLD.1)

The developer shall provide the low-level design of the TSF.[ADV_LLD.1.1D]

The presentation of the low-level design shall be informal.[ADV_LLD.1.1C]

The low-level design shall be internally consistent.[ADV_LLD.1.2C]

The low-level design shall describe the TSF in terms of modules.[ADV_LLD.1.3C]

The low-level design shall describe the purpose of each module.[ADV_LLD.1.4C]

The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.[ADV_LLD.1.5C]

The low-level design shall describe how each TSP-enforcing function is provided.[ADV_LLD.1.6C]

The low-level design shall identify all interfaces to the modules of the TSF.[ADV_LLD.1.7C]

The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.[ADV_LLD.1.8C]

The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.[ADV_LLD.1.9C]

The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.[ADV_LLD.1.10C]

6.2.3.6 Informal correspondence demonstration

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.[ADV_RCR.1.1D]

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.[ADV_RCR.1.1C]

6.2.3.7 Informal TOE security policy model

The developer shall provide a TSP model.[ADV_SPM.1.1D]

The developer shall demonstrate correspondence between the functional specification and the TSP model.[ADV_SPM.1.2D]

The TSP model shall be informal.[ADV_SPM.1.1C]

The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.[ADV_SPM.1.2C]

The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.[ADV_SPM.1.3C]

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.[ADV_SPM.1.4C]

6.2.4 Guidance document

6.2.4.1 Administrator guidance (AGD_FSP.1)

The developer shall provide administrator guidance addressed to system administrative personnel.[AGD_ADM.1.1D]

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.[AGD_ADM.1.1C]

The administrator guidance shall describe how to administer the TOE in a secure manner.[AGD_ADM.1.2C]

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.[AGD_ADM.1.3C]

The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.[AGD_ADM.1.4C]

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.[AGD_ADM.1.5C]

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.[AGD_ADM.1.6C]

The administrator guidance shall be consistent with all other documentation supplied for evaluation.[AGD_ADM.1.7C]

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.[AGD_ADM.1.8C]

6.2.4.2 User guidance (AGD_USR.1)

The developer shall provide user guidance.[AGD_USR.1.1D]

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.[AGD_USR.1.1C]

The user guidance shall describe the use of user-accessible security functions provided by the TOE.[AGD_USR.1.2C]

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.[AGD_USR.1.3C]

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.[AGD_USR.1.4C]

The user guidance shall be consistent with all other documentation supplied for evaluation.[AGD_USR.1.5C]

The user guidance shall describe all security requirements for the IT environment that are relevant to the user.[AGD_USR.1.6C]

6.2.5 Life cycle support (ALC)

6.2.5.1 Identification of security measures (ALC_DVS.1)

The developer shall produce development security documentation.[ALC_DVS.2.1D]

The development security documentation shall describe all the physical,procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.[ALC_DVS.2.1C]

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.[ALC_DVS.2.2C]

The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.[ALC_DVS.2.3C]

6.2.5.2 Life cycle definition (ALC_LCD.1)

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.[ALC_LCD.1.1D]

The developer shall provide life-cycle definition documentation.[ALC_LCD.1.2D]

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.[ALC_LCD.1.1C]

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.[ALC_LCD.1.2C]

6.2.5.3 Well-defines development tools (ALC_TAT.1)

The developer shall identify the development tools being used for the TOE.[ALC_TAT.1.1D]

The developer shall document the selected implementation-dependent options of the development tools.[ALC_TAT.1.2D]

All development tools used for implementation shall be well-defined.[ALC_TAT.1.1C]

The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.[ALC_TAT.1.2C]

The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.[ALC_TAT.1.3C]

6.2.6 Tests (ATE)

6.2.6.1 Analysis of coverage (ATE_COV.2)

The developer shall provide an analysis of the test coverage.[ATE_COV.2.1D]

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.[ATE_COV.2.1C]

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.[ATE_COV.2.2C]

6.2.6.2 Testing: high-level design (ATE_DPT.1)

The developer shall provide the analysis of the depth of testing.[ATE_DPT.1.1D]

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

6.2.6.3 Functional Testing (ATE_FUN.1)

The developer shall test the TSF and document the results.[ATE_FUN.1.1D]

The developer shall provide test documentation.[ATE_FUN.1.2D]

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.[ATE_FUN.1.1C]

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.[ATE_FUN.1.2C]

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.[ATE_FUN.1.3C]

The expected test results shall show the anticipated outputs from a successful execution of the tests.[ATE_FUN.1.4C]

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.[ATE_FUN.1.5C]

6.2.6.6 Independent testing - sample (ATE_IND.2)

The developer shall provide the TOE for testing.[ATE_IND.2.1D]

The TOE shall be suitable for testing.[ATE_IND.2.1C]

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.[ATE_IND.2.2C]

6.2.7 Vulnerability assessment (AVA)

6.2.7.1 Validation of analysis (AVA_MSU.2)

The developer shall provide guidance documentation.[AVA_MSU.2.1D]

The developer shall document an analysis of the guidance documentation.[AVA_MSU.2.2D]

The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.[AVA_MSU.2.1C]

The guidance documentation shall be complete, clear, consistent and reasonable.[AVA_MSU.2.2C]

The guidance documentation shall list all assumptions about the intended environment.[AVA_MSU.2.3C]

The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).[AVA_MSU.2.4C]

The analysis documentation shall demonstrate that the guidance documentation is complete.[AVA_MSU.2.5C]

6.2.7.2 Strength of TOE security function evaluation

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.[AVA_SOF.1.1D]

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.[AVA_SOF.1.1C]

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.[AVA_SOF.1.2C]

6.2.7.3 Developer vulnerability analysis (AVA_VLA.1)

The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.[AVA_VLA.1.1D]

The developer shall document the disposition of obvious vulnerabilities.[AVA_VLA.1.2D]

The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.[AVA_VLA.1.1C]

7 Rationale

This section provides the rationale for the selection, creation, and use of the security policies, threats, objectives, and functional requirements components

7.1 Security Objectives Rationale

The goal of this section is to demonstrate that the objectives of this PP are sufficient to counter the identified threats and supports the identified assumptions. Table 7.1 provides a summary mapping of threats, assumptions and the objectives.

Assumptions	Objectives
A.Host_Platform	OE.Host_Platform
A.No_MLS_Operation	OE.Host_Operation
A.Authentication_Token	OE.Authentication_Token
A.TOE_Transparency	OE.TOE_Transparency
A.Network	OE.Network
A.Physical_Protection	OE.Physical_Protection
Threat	Objectives
T.Admin	O.Audit, O.Audit_Management, O.Management, OE.User_Trust, OE.Training
T.Admin_Role	O.Management, O.Single_Factor_Authentication, O.Audit
T.Domain_Isolation	O.Single_Domain, O.Information_Isolation, O.Cryptographic_Services, O.Information_Reuse, O.Periods_Processing,O.Policy_Enforcement
T.Implementation	O.TSF_Implementation
T.Information_Flow	O.Cryptography, O.Trusted_Communication, O.Cryptographic_Services, O.Information_Isolation
T.TOE_Failure	O.Fail_Secure
T.TSF_Bypassibility	O.TSF_Non_Bypassability
T.TSF_Integrity	O.TSF_Integrity, O.TSF_Protection

T.Unauthorized_TOE_Access	O.Domain_Participation_Authentication
T.Untrusted_Communication	O.Trusted_Communication
OSP	**Objectives**
P.Authentication_Credentials	O.Credentials, OE.Autentication_Credentials
P.Policy_Violation_Alert	O.Audit, O.Audit_Management, O.Audit_Review_Notification, O.Immediate_Violation_Notification
P.Strong_Authentication	O.Domain_Participation_Authentication
P.Training	OE.Training
P.Trusted_User	OE.Trusted_User
P.Cryptography	O.Cryptographic_Services, O.Cryptography
P.Credential_Protection	O.TSF_Protection, OE_Credential_Protection

Table7-1. Security Environment-to-Security Objective Mapping

7.1.1 Threats

T.Admin
This threat is addressed by the following objectives:

O.Audit

This objective counters T.Admin by requiring the TOE to be able to record security events performed by administrators; to associate the identity of the individual that operates as an administrator with each event recorded; and to record sufficient information to support follow-up action.

O.Audit_Management

This objective counters T.Admin by requiring the TOE to implement a capability to review the audit trail for events created by administrators.

O.Management

This objective counters T.Admin by requiring the TOE be capable of configuring the audit trail to record the security relevant events performed by administrators.

OE.User_Trust

This objective counters T.Admin by requiring administrators to be made aware of their responsibilities as administrators and to properly manage/configure/operate the TOE in accordance with policy/procedures.

OE.Training

This objective counters T.Admin by requiring administrators to be trained in the proper use and operation of the TOE and to understand their responsibilities as administrators and to properly manage/configure/operate the TOE in accordance with policy/procedures

T.Admin_Role

This threat is addressed by the following objectives:

O.Management

This objective counters T.Admin_Role by requiring the TOE to have functions that may be invoked only by individuals with appropriate administrative authorizations.

O.Single_Factor_Authentication

This objective counters T.Admin_Role by providing an authentication mechanism that authenticated individuals as authorized administrators. The mechanism then provides these individuals the authorizations required to invoke administrative functions.

T.Domain_Isolation

This threat is addressed by the following objectives:

O.Single_Domain

This objective counters the Bridge aspect of T.Domain_Isolation by preventing the TOE/user pair from simultaneous participation in more than one domain at a time.

O.Information_Isolation

This objective counters T.Domain_Isolation by implementing and enforcing the DIFP information flow control policy. The DIFP establishes the criteria for allowed and disallowed information flows and the TSF enforces the criteria on a domain by domain basis.

O.Cryptographic_Services

This objective counters the Cryptography of T.Domain_Isolation by invoking the correct cryptographic service as defined by the DIFP.

O.Information_Reuse

This objective counters the object reuse aspect of T.Domain_Isolation by requiring all components except for the host component to ensure that the residual domain information content contained in an allocated storage location is not available after domain session changes.

O.Periods_Processing

This objective counters T.Domain_Isolation by ensuring that within the TOE host component volatile hardware/firmware, residual information associated with a terminated domain session is not available upon establishment of a new domain session.

O.Policy_Enforcement

This objective counters the T.Domain_Isolation by requiring personalities to be defined for individuals and for each TOE instance, and by defining an information flow control policy that is associated with an individual/TOE pair through their respective personalities; and through the enforcement of the DIFP selected by the individual once they are authenticated. The Policy_Enforcement aspect of T.Domain_Isolation is countered by ensuring that the criteria for unauthorized information flows is defined and enforced.

T.Implementation

This threat is countered by the following objectives:

O.Implementation

This objective counters T.Implementation by requiring that design documentation be developed in accordance with the requirements of the EAL4 ADV components; that testing be accomplished in accordance with EAL4 ATE components, and that misuse and vulnerability assurance is obtained via the EAL4 AVA components.

T.Information_Flow

This threat is countered by the following objectives:

O.Cryptography

O.Cryptography counter T.Information_Flow as stated in the following discussion. The objective counter the Intercept aspect of T.Information_Flow not by preventing intercept of information flow, but by requiring sufficiently strong encryption to minimize the likelihood that any intercepted information may be deciphered and utilized.

The objective counter the Substitution aspect of T.Information_Flow by providing integrity services that make it possible for the receiver of an information flow to determine that a received information flow has been modified subsequent to its transmission by the sender.

The objective counter the Interject aspect of T.Information_Flow by providing cryptographic services that support allowing the sending and receiving TSFs of an information flow to establish a mutual trust relationship prior to initiating any information flow between them.

O.Trusted_Communication

This objective counters the Interject aspect of T.Information_Flow by requiring that mutual authentication between two communicating TOEs occur prior to any information flow occurring between the TOEs. The mutual authentication is based upon cryptographic services to minimize the likelihood that an untrusted device is able to communicate with the TOE.

O.Cryptographic_Services

This objectives counters T.Information_Flow by requiring the TOE to be able to associate and employ the appropriate mechanisms as specified by the DIFP.

O.Information_Isolation

This objective counters T.Information_Flow by implementing and enforcing the DIFP information flow control policy. The DIFP establishes the criteria for establishing the trust relationship between two communicating TOE instances as well as the criteria for allowing and implementing information flows. The TSF enforces these criteria for every TOE-to-TOE communication session.

T.TOE_Failure

This threat is addressed by the following objectives:

O.Fail_Secure

This objective counter T.TOE_Failure by requiring the TSF to fail securely such that information flows are disabled upon detection of any condition that would prevent the TOE from functioning properly.

T.TSF_Bypassibility

This threat is addressed by the following objectives:

O.TSF_Non_Bypassability

If the TSF can be bypassed, then (unauthorized) access to protected objects and resources may occur despite the correct design and implementation of the policy enforcement aspects of the TSF. This objective counters T.TSF_Bypassibility by requiring the TSF to always be invoked and for the TSF to succeed (i.e. return a grant/allow decision) for each event that requires TSF-mediation.

T.TSF_Intensity

This threat is addressed by the following objectives:

O.TSF_Intensity

This objective counters T.TSF_Integrity by requiring the TSF to incorporate self-test and other diagnostic mechanisms capable of detecting any change or alteration to the TSF, such that the TOE may be halted to prevent continued operation in a potentially unsecure state.

O.TSF_Protection

This objectives counters T.TSF_Integrity by requiring the TSF to be designed and implemented to protect itself from access by untrusted individuals and processes.

T.Unauthorized_TOE_Access

This threat is addressed by the following objectives:

O.Domain_Participation_Authentication

This objective counters T.Unauthorized_TOE_Access by requiring the TOE to employ two-factor strong authentication mechanisms as the basis for authenticating the claimed identity of individuals wishing to participate in a domain. In addition, this objective requires that the individual user/TOE pair be a factor in the domain participation authentication to ensure they are both authorized to join the requested domain.

T.Untrusted_Communication

This threat is addressed by the following objectives:

O.Trusted_Communication

This objective counters T.Untrusted_Communication by requiring each TOE-to-TOE domain communication to be based upon a TOE-to-TOE mutually authenticated trust relationship. This trust relationship must be established prior to allowing information flows to occur between two instances of the TOE.

7.1.2 Organisational Security Policies (OSPs)

P.Authentication_Credentials

This policy is addressed by the following objectives:

O.Credentials

This objective enforces P.Authentication_Credentials by requiring the TOE to have the capability of managing the credentials used to authenticate discrete TOE instances, to establish TOE-to-TOE trust relationships, and to authenticate individual TOE users and administrators.

OE.Authentication_Credentials

This objective enforces P.Authentication_Credentials by requiring that the organization with responsibility for employing the TOE establish the appropriate procedures and mechanisms to develop, distribute, and control the authentication credentials used by the TOE and individual users and administrators of the TOE

P.Policy_Violation_Alert

This policy is addressed by the following objectives:

O.Audit

This objective enforces P.Policy_Violation_Alert by requiring the TOE to have the capabilility to record all violations of enforced policies performed by the user and/or administrators.

O.Audit_Management

This objective enforces P.Policy_Violation_Alert by requiring the TOE to have the capability to review the audit trail for events created by administrators.

O.Audit_Review_Notification

This objective enforces P.Policy_Violation_Alert by requiring the TOE to have the capability to provide notification to the appropriate administrative personnel of review violations of enforced policy detected during the review of the auditable events created.

O.Immediate_Violation_Notification

This objective enforces P.Policy_Violation_Alert by requiring the TOE to have the capability to provide immediate notification of a violation of enforced policy of to the administrative personnel.

P.Strong_Authentication

This policy is addressed by the following objectives:

O.Domain_Participation_Authentication

This objective enforces P.Strong_Authentication by requiring the TOE to employ at least one two-factor strong authentication mechanism as the basis for authenticating the claimed identity of individuals wishing to participate in a domain.

P.Training

This policy is addressed by the following objectives:

OE.Training

This objective enforces P.Training by ensuring that all users are properly instructed on policies and procedures for using the system, as well as, being able to acknowledge all threats and vulnerabilities that may impact system processing

P.Trusted_User

OE.Trusted_User

This objective enforces P.Trusted_User by ensuring that the all trusted users adherence to policies, procedures, system, admin, and user documentation, associated with the TOE and all systems that interface with the TOE.

P.Crypography

This policy is addressed by the following objectives:

O.Cryptographic_Services

This objective enforces P.Cryptography by requiring the TSF to be able to maintain appropriate information to correctly correlate and employ cryptographic services as specified by governing policy.

O.Cryptography

This objective enforces P.Cryptography by requiring the TSF to interface with accredited cryptographic services and to employ these services as specified by governing policy.

P.Credential_Protection

O.TSF_Protection

This objective enforces P.Credential_Protection by requiring the TSF to implement protections to prevent unauthorized access to authentication credentials while they are within the scope of control of the TSF.

1590 OE_Credential_Protection

This objective enforces P.Credential_Protection by requiring individual users and administrators of the TOE to protect authentication credentials to prevent unauthorized access while they are in their possession.

1595 7.2 Security Functional Requirement Rationale

The goal of this section is to demonstrate that the objectives of this PP are addressed by the functional and assurance requirement components. Table 7-2 summaries how each functional and assurance requirement serves to address the objective of this profile.

Objectives	Requirements
TOE Security Objectives	
O.Audit	FAU_GEN.1.1, FAU_GEN.1.2, FAU_GEN.2.1, FPT_STM.1.1, FIA_UID.1.1
O.Audit_Management	FAU_SAR.1.1, FAU_SAR.1.2, FAU_SAR.3.1, FAU_SEL.1.1, FMT_MTD.1.1
O.Audit_Protection	FAU_SAR.2.1,
O.Audit_Review_Notification	FAU_SAA.1.1, FAU_SAA.1.2, FAU_ARP.1.1
O.Credential	FAU_SAR.2.2, FMT_MSA.1.1, FMT_MSA.1.2, FMT_MTD.1.1 (these are questionable)

O.Cryptographic_Services	FCS_COP.1.1; FCS_CKM.1.1, FCS_CKM.4.1, FMT_MSA.2, FMT_MSA.3.1
O.Domain Isolation	TDB
O.Domain_Participation_Authentication	FIA_UAU.5.1, FIA_UAU.5.2., FIA_UID.2.1
O.Fail_Secure	TDB
O.Immediate_Violation_Notification	FAU_SAA.1.1, FAU_SAA.1.2, FAU_ARP.1.1
O.Information_Isolation	FDP_IFC.1.1; FDP_IFF.1.1; FDP_IFF.1.2, FDP_IFF.1.3, FDP_IFF.1.4, FDP_IFF.1.5, FDP_IFF.1.6
O.Information_Reuse	FDP_RIP.1.1
O.Management	FIA_UAU.2.1, FMT_REV.1.1; FMT_REV.1.2, FMT_SMR.1.1, FMT_SMR.1.2
O.Policy_Enforcement	FDP_ACC.1.1, FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3, FDP_ACF.1.4, FMT_MSA.3.1, FDP_IFC.1.1, FDP_IFF.1.1; FDP_IFF.1.2, FDP_IFF.1.3, FDP_IFF.1.4, FDP_IFF.1.5 FDP_IFF.1.6
O.Single_Domain	FIA_UAU.5.1, FIA_UAU.5.2, FTA_MCS.1,1, FT1_MCS.1.2

O.Single_Factor_ Authentication	TBD
O.Trusted_Communication	FPT_ITC.1.1, FTP_ITC.1.2, FTP_ITC.1.3
O.TSF_Implementation	Assurance Requirements.
O.TSF_Integrity	FPT_AMT.1.1, FPT_TST.1.1, FPT_TST.1.2, FPT_TST.1.3
O.TSF_Non_Bypassability	FPT_RVM.1.1
O.TSF_Protection	FAU_SAR.2.2, FMT_MSA.1.1, FMT_MSA.1.2, FMT_MTD.1.1, FPT_SEP.2.1, FPT_SEP.2.2, FPT_SEP.2.3
O.Type1_Cryptography	FCS_COP.1.1, FCS_CKM.1.1, FCS_CKM.4.1, FMT_MSA.2
O.Type2_Cryptography	FCS_COP.1.1, FCS_CKM.1.1, FCS_CKM.4.1, FMT_MSA.2
Assurance Requirements	
Security Objectives	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2, ADO_DEL.2, ADO_IGS.1, ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1, AGD_ADM.1 AGD_USR.1, ALC_DVS.1, ALC_LCD.1 ALC_TAT.1, ATE_COV.2, ATE_DPT.1 ATE_FUN.1, ATE_IND.2, AVA_MSU.2 AVA_SOF.1, AVAVLA.2

Appendix A. Concept of Operation

Appendix A is provided to reiterate the essential functionality of the TOE, using simplistic techniques adapted from the "Use Case" feature of the "Unified Modeling Language (UML)." This appendix may be omitted by those individuals who have a firm understanding of the concepts addressed within the MDS PP. It may be useful to others who may want to present these functional capabilities of the TOE via high level abstractions in briefings.

A.1 Objects in TOE Operational Environment

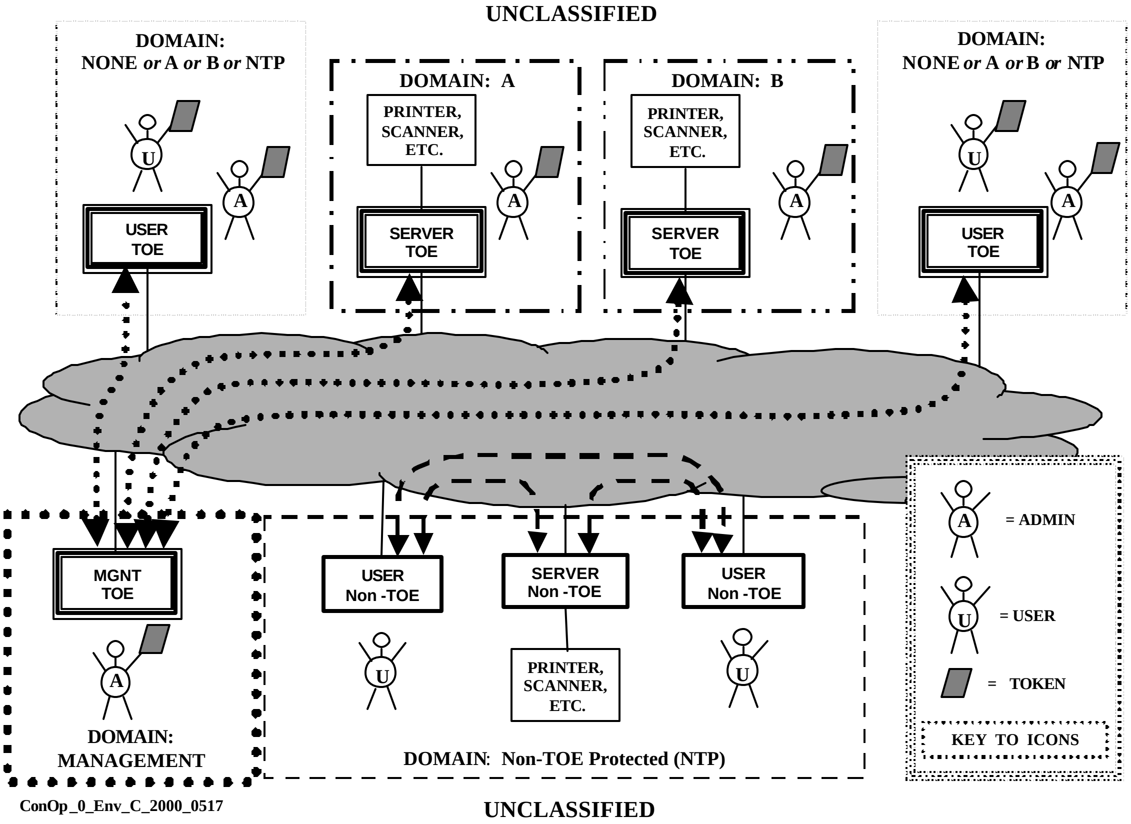


Figure A-1: Objects in TOE Operational Environment.

Figure A-1 introduces all of the types of symbology used in figures of this sub-section to depict particular operational scenarios of the TOE.

A.1.1 TOE

Recall that the TOE consists of the following abstract components:

- Host Component;
- Network Interface Component;
- User Component;
- Management Component; and
- Credential Input Component.

Instances of the TOE are indicated by rectangles with concentric borders. Though the instances of the TOE are all identical, they are captioned differently in the figure to distinguish between three applications / roles of the TOE:

- User Workstation – may be used by one or more personnel, one at a time.
- Server -- may function as a file server, host a web server, etc., as well as drive shared peripheral devices.
- TOE Management – may be either static and centralized (as shown), decentralized, or dynamically assigned.

TOE Management is shown here as a TOE dedicated to centralized management. This roll may instead be distributed over multiple instances of the TOE, and thus not involve a particular Management TOE.

A.1.2 Token

The Token is the only part (not component) of the TOE which is shown outside the TOE rectangle, since it is issued to and associated with a particular User or Administrator, and these personnel are indeed mobile.

A.1.3 Domains

Three representative domains are depicted, namely Domain "A", Domain "B", and the "Non-TOE Protected (NTP)" Domain. Workstations, servers, instances of the TOE, peripheral devices, and personnel operating in each particular domain are enclosed by a rectangular border decorated with a distinctive modulation dedicated to the domain.

A.1.4 Network Cloud

The network cloud represents a logically contiguous networking topology that may range from a single LAN segment to multiple LANs connected via a WAN. It may include wired, fiber optic, radio, and optical links. No physical protection of these communications paths is assumed.

A.1.5 Communications

Modulated lines with double arrowheads, which pass through the network cloud, are used to indicate communications. The heavy dotted lines in Figure A-1 represent TSF management communications between each powered-up instance of the TOE and the TOE Management component. These communications are used for services such as Audit Collection and TOE health monitoring. To reduce clutter, they are not shown on the operational scenarios, though they continue to exist. Note that their decorative modulation corresponds to the modulation in the border around the "Management TOE." Likewise, the communications of the Non-TOE Protected workstations and server are modulated like the border of their special domain. This convention will also be used for Domain "A" and for Domain "B" communications.

A.1.6 Personnel

Both User Personnel and Administrative Personnel are depicted wearing nice tee shirts proclaiming their roles. These tee shirts are a step up from the UML stick man convention. This diagram shows them at all the places in which they will perform their roles.

A.1.7 Peripheral Devices & Network Devices

Printers, scanners, and similar devices are depicted as driven from "Server TOE" instances, or by Non-TOE Protected Servers. Since the TOE incorporates a Host Component, per this profile, devices such as network printers are not addressed.

A.2 TOE Deployment and Initialization

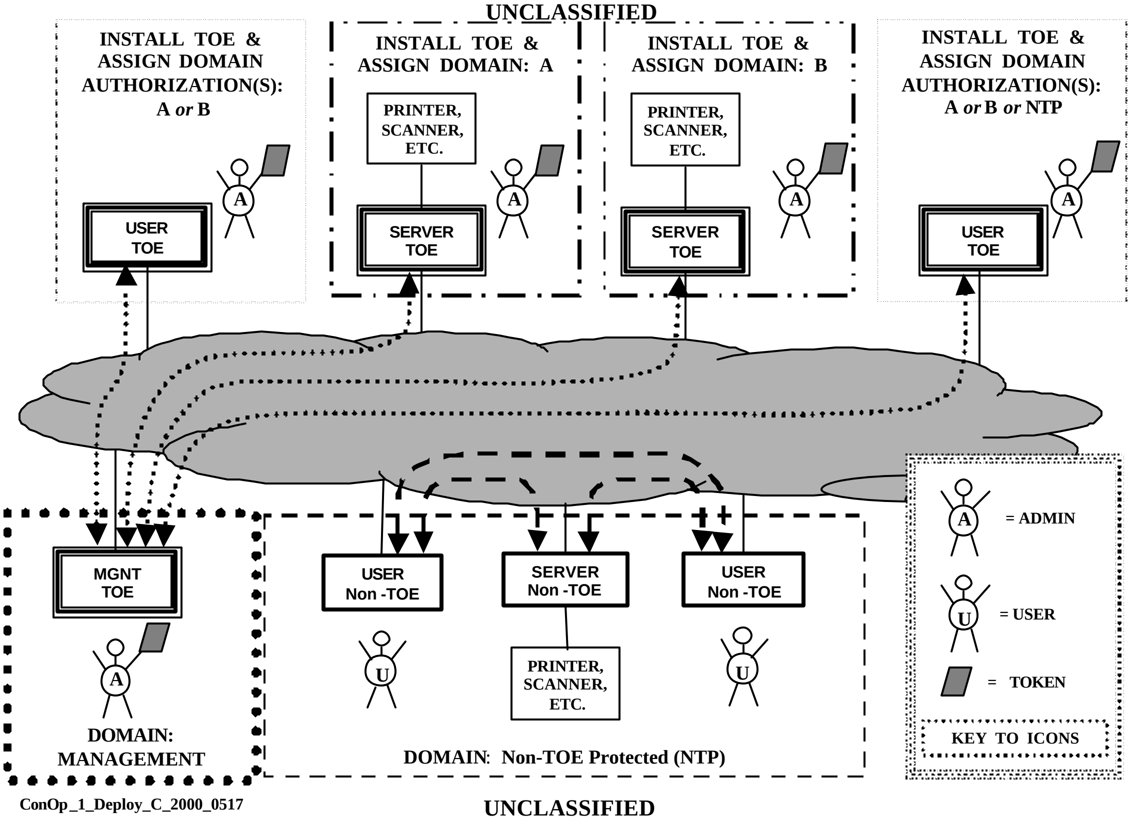

UNCLASSIFIED
INSTALL TOE & ASSIGN DOMAIN AUTHORIZATION(S): A or B
INSTALL TOE & ASSIGN DOMAIN: A
INSTALL TOE & ASSIGN DOMAIN: B
INSTALL TOE & ASSIGN DOMAIN AUTHORIZATION(S): A or B or NTP
PRINTER, SCANNER, ETC.
PRINTER, SCANNER, ETC.
USER TOE
SERVER TOE
SERVER TOE
USER TOE
A
MGNT TOE
USER Non -TOE
SERVER Non -TOE
USER Non -TOE
PRINTER, SCANNER, ETC.
U
DOMAIN: MANAGEMENT
DOMAIN: Non-TOE Protected (NTP)
= ADMIN
= USER
= TOKEN
KEY TO ICONS
ConOp_1_Deploy_C_2000_0517
UNCLASSIFIED

Figure A-2: TOE Deployment and Initialization.

Figure A-2 depicts the deployment and initialization of TOEs on an already existing network. Users and administrative personnel already using the pre-existing network, whose equipment is not retrofitted with instances of the TOE, are considered to inhabit the "Non-TOE Protected (NTP) Domain." They may continue to operate in that domain during and after the process of TOE deployment and initialization.

Deployment and initialization of the TOE is at least a two-part process. The order in which these processes are performed may or may not be of importance, depending upon the design of the TOE.

A.2.1 TOE Management Component

Administrative personnel translate organizational policies into the TOE's *Domain Information Flow Policy (DIFP).* The set of possible TOE Personalities is defined in accordance with the DIFP. Each particular TOE's Profile is constructed in accordance with the DIFP by assembly of a set of zero or more personalities with which it can be authorized to operate. These personalities are selected from the set of all possible TOE Personalities. The TOE Profiles used in this example are depicted in Table A-2a. In this table, the italicized words *"Left"* and *"Right"* refer to the physical positioning of the corresponding TOEs in the set of diagrams used in this section.

Personality (Domain in which a TOE can be authorized to participate)	**Profiles of TOE Instances in Diagrams**				
	Management TOE	***Left*** **User TOE**	***Left*** **Server TOE**	***Right*** **Server TOE**	***Right*** **User TOE**
Management	**X**	**X**	**X**	**X**	**X**
A		**X**	**X**		**X**
B		**X**		**X**	**X**
NTP					**X**

Table A-2a. Profiles of TOE Instances in Diagrams

There are three types of personalities/domains of operation represented in this table:

- Management – A special domain in which all TOEs participate. It may or may not involve TOE to TOE communication, depending on whether the Management Component is distributed or centralized.
- Specific Domain – Domains such as "A" or "B" in which isolated information is to be exchanged. Notice that a TOE, such as the *Right* **User TOE** may be granted personalities for participation in all domains known to the Management Component. A TOE with all of the available personalities may be thought of as a "Wild Card TOE."
- NTP – The Non-TOE Protected Domain in which non-TOE-equipped hosts operate and communicate via the network. Note that a TOE-equipped-host must be granted a personality specific to this special domain, in order to be eligible to gain participation in this special domain.

Since a TOE can exhibit at most one personality at a time, it may participate in at most one domain at a time.

The Periods Processing Host Component of the TOE may be able to be used in a Stand-alone mode, without authentication by the TOE. This is not a domain, but a mode in which a TOE equipped host may operate without interaction via the network.

A.2.2 TOE Installation and Configuration

Administrative personnel are depicted installing instances of the TOE, and configuring these TOEs for proper operation on the network. After this configuration, each installed instance of the TOE shall have, at a minimum, a unique identification on the network. Association of an instance of the TOE and its profile is performed by the TOE Management Component.

The modulated lines in Figure A-2 indicating communications with the TOE Management Component indicate any required initialization events. These modulated lines also indicate the communications by which Administrators perform strong authentication with the TOE Management Component.

A.2.3 Server TOE Start-Up

Administrator personnel also assist the two Server TOEs, one dedicated to Domain A and one dedicated to Domain B, to begin participation in their respective domains. Once these Server TOEs have joined domains, they may continue to operate in these domains as long as they are powered up. The Administrator may or may not be required to leave a token at a server TOE in order for it to operate unattended, depending on how the TOE is designed.

A.3 User Enrolment

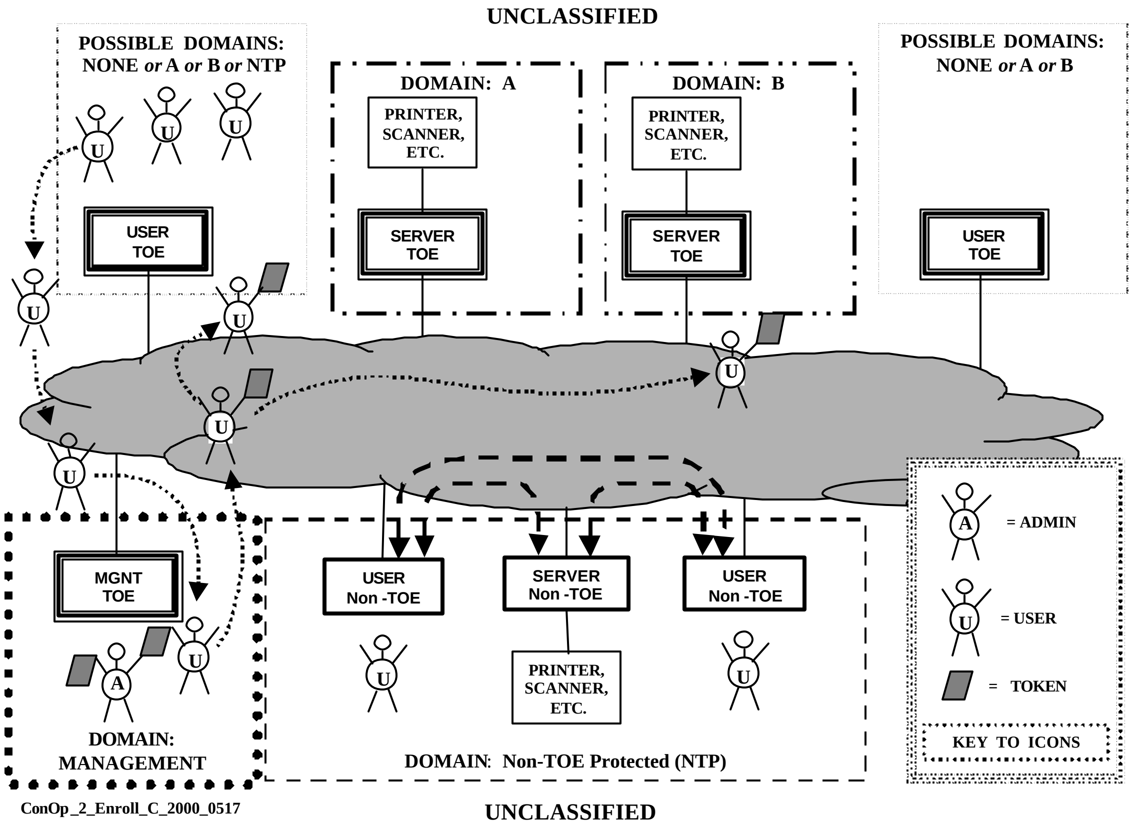


Figure A-3: User Enrolment.

1720 Figure A-3 depicts the process of User Enrollment. It entails generation of credentials and issuance of hardware tokens to the new Users. The users are to use these tokens as one factor in two part strong authentication of the user to the TOE. The other factor for use in this authentication is TOE design specific, and may be a password, PIN, biometric measurement, or some other factor.

1725 In this depiction, the candidate users visit the TOE Administrator to be enrolled and to receive their tokens. This physical visit may or may not required, depending upon the design of the TOE. It will likely be required if the taking of some biometric measurement is needed for enrollment. If biometrics are not used, enrollment requests might be provided to the Administrator via some other means, and Tokens and passwords shipped to the new users via separate paths.

1730 Another part of this process is the generation and storage of a profile for the user. A User's profile is composed of one or more personalities, which the user can subsequently employ in interaction with the TOE. Each personality defines a domain in which the user can be authenticated to participate. It can also impose a variety of restrictive conditions on the user's actions in the domain.

1735 A.4 TOE Operation: Upper Left User in Domain "A" and Upper Right User in Domain "B"

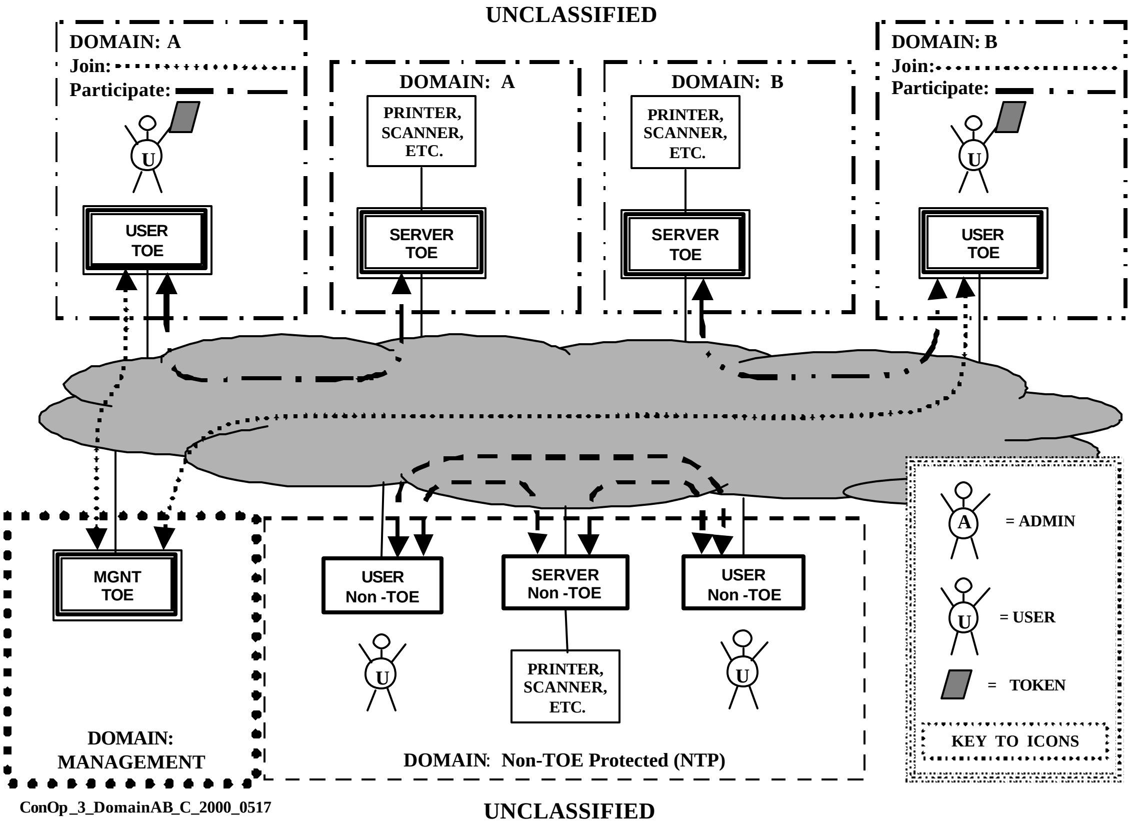


Figure A-4: Upper Left User in Domain "A" & Upper Right User in Domain "B."

Figure A-4 depicts the operation of users in all of the three potential domains used in this set of 1740 scenarios. The users in the Non-TOE Protected (NTP) domain are simply continuing their operations as they did before TOE deployment.

The user shown at the Upper Left User TOE has been granted participation in (gained operational access to) Domain "A" by satisfaction of several requirements:

- His TOE's Host Component had properly passed through its information neutral state.
- 1745 He had successfully accomplished strong (two part) authentication with the TOE Management Component from the TOE which he is shown to be using. In addition to the TOE Management Component, this required his use of at least his Token, his second, implementation specific, authentication part, the TOE Credential Input Component, and the TOE User Component.
- 1750 The User TOE he is using had been authorized to participate in Domain "A".

- He has a valid (i.e. non-expired, non-revoked) Domain "A" user personality as one part of his profile.
- His Domain "A" user personality authorizes his use of the Upper Left User TOE, in Domain "A", at the current time of day, and day of the week / month / etc.

Once the user shown at the Upper Left User TOE has gained participation in (joined) Domain "A", he may then continue to participate in this domain as long as the following remain true:

- His Domain "A" User personality has not been changed or revoked via the TOE Management Component
- Time has not progressed to some point at which he is not authorized to use this Domain "A" personality at this particular User TOE.
- His User TOE has remained powered up and operating properly.

While this Upper Left User is participating in Domain "A", in this scenario, he may logically interact with only the Domain "A" Server, since no other TOE, in addition to his and the server's TOE, are participating in Domain "A". He can thus send e-mail to be stored on the Domain "A" e-mail server, retrieve his Domain "A" e-mail from it, and interact with any file server, web server, print server, or etc. which the Domain "A" server may provide.

When the Upper Left User has completed his work in Domain "A", he shall log off from the domain, and from his User TOE. The Host Component of the User TOE that he had used shall then enter its sanitized state. The definition of User, however, either as an individual, or as more than one individual who are to share a Roll, is dependent upon organizational policy. It may thus be permissible for an individual to hand over operation of a TOE to another individual, who is to continue its use in the same domain, while performing the same Roll, without the logoff, neutral state, logon process. This requirement can arise in operational scenarios in which operational downtime between individuals who are to perform the same roll cannot be tolerated.

This same discussion is applicable to the Upper Right User, and his use of a TOE in Domain "B". Again, in this figure, the only operational communications which he may make are with the Domain "B" server.

Note that the communications in TOE Protected Domains are depicted with lines modulated in a way specific to each domain.

A.5 TOE Operation: Both Upper Left User and Upper Right User in Domain "B"

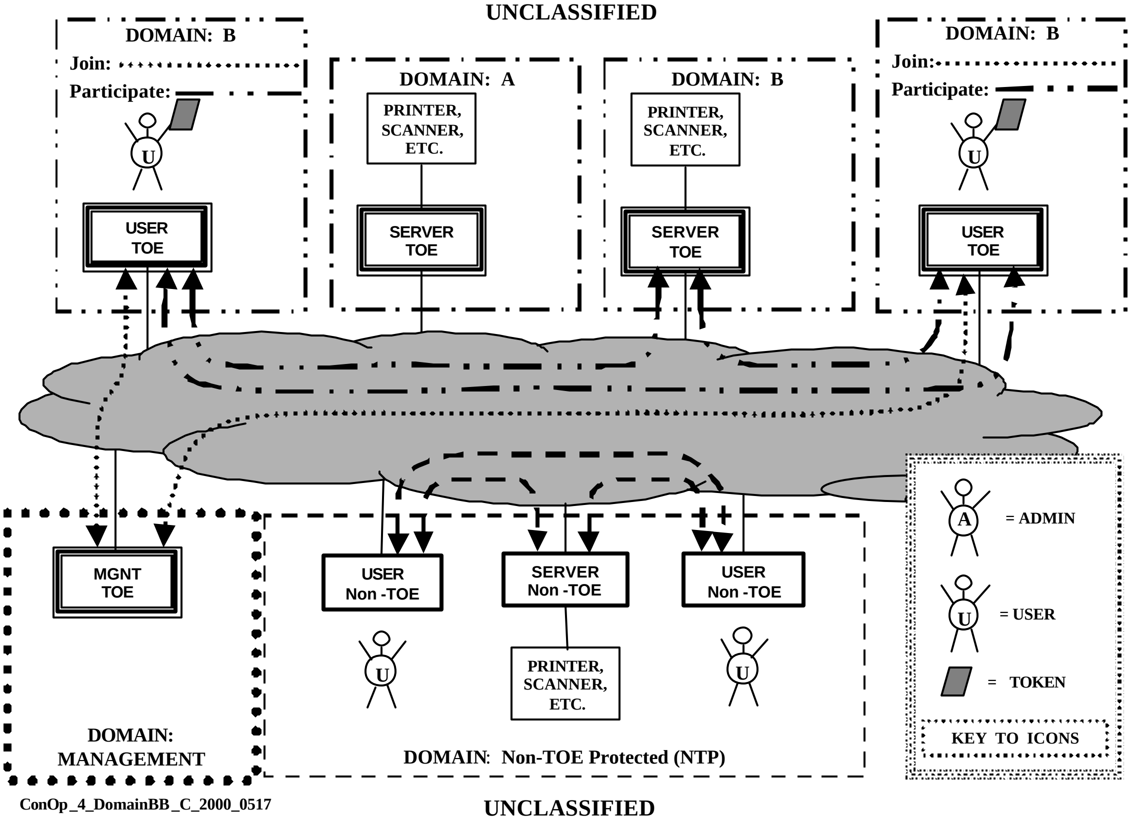


Figure A-5: Both Upper Left User & Upper Right User in Domain "B."

Figure A-5 depicts the operation of users in two of the three potential domains used in this set of
1785 scenarios. The users in the Non-TOE Protected (NTP) domain are simply continuing their
operations as they did before TOE deployment.

Both the user shown at the Upper Left User TOE and the User at the Upper Right User TOE
have joined (gained operational access to) Domain "B" by satisfaction of several requirements as
was discussed for the previous scenario. Conditions for continued participation in this domain,
1790 and Log Off requirements for the Upper Left User and the Upper Right User are also as they
were for the previous scenario.

While these Upper Left and Upper Right Users are participating in Domain "B", they may
logically interact with the Domain "B" Server. If their TOEs are authorized to communicate
directly with each other, while in Domain "B", they will also be capable of direct interaction (e.g.
1795 perhaps FTP, sharing of files on their local drive, etc.).

Note that the communications in TOE Protected Domains are depicted with lines modulated in a way specific to Domain "B."

A.6 TOE Operation: Upper Left User Standalone and Upper Right User in Domain "A"

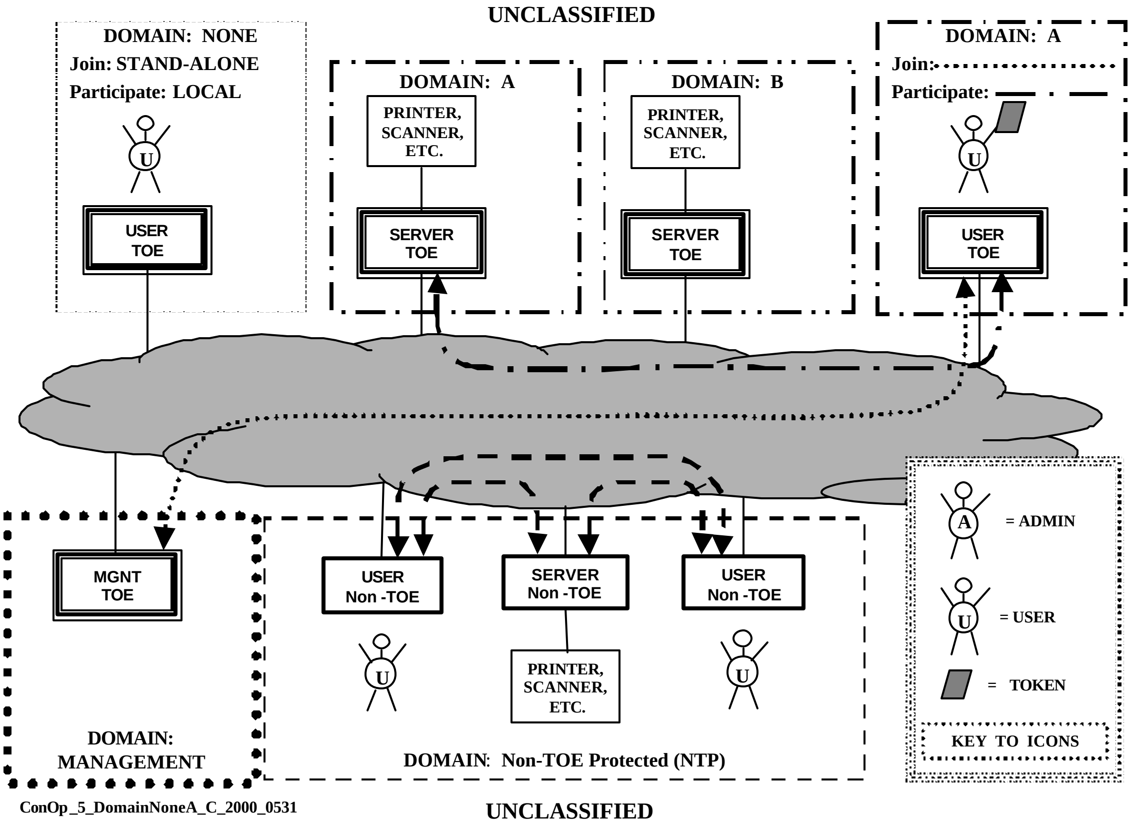


Figure A-6: Upper Left User "Standalone" & Upper Right User in Domain "A."

Figure A-6 depicts the operation of users in two of the three potential domains used in this set of scenarios. The users in the Non-TOE Protected (NTP) domain are simply continuing their operations as they did before TOE deployment.

Requirements for the User at the Upper Right User TOE, who has joined Domain "B", are as they were in the previous scenarios.

Note that there is a User operating the Upper Left TOE in a Standalone mode. That TOE is not a member of any domain.

While the Upper Right User is participating in Domain "A", in this scenario, he may logically interact with only the Domain "A" Server, since no other TOE, in addition to his and the server's TOE, are participating in Domain "A". He can thus send e-mail to be stored on the Domain "A" e-mail server, retrieve his Domain "A" e-mail from it, and interact with any file server, web server, print server, or etc. which the Domain "A" server may provide.

The communications in TOE Protected Domains are depicted with a line modulated in a way specific to Domain "A."

A.7 TOE Operation: Upper Left User in Domain "A" & Upper Right User in Domain "NTP"

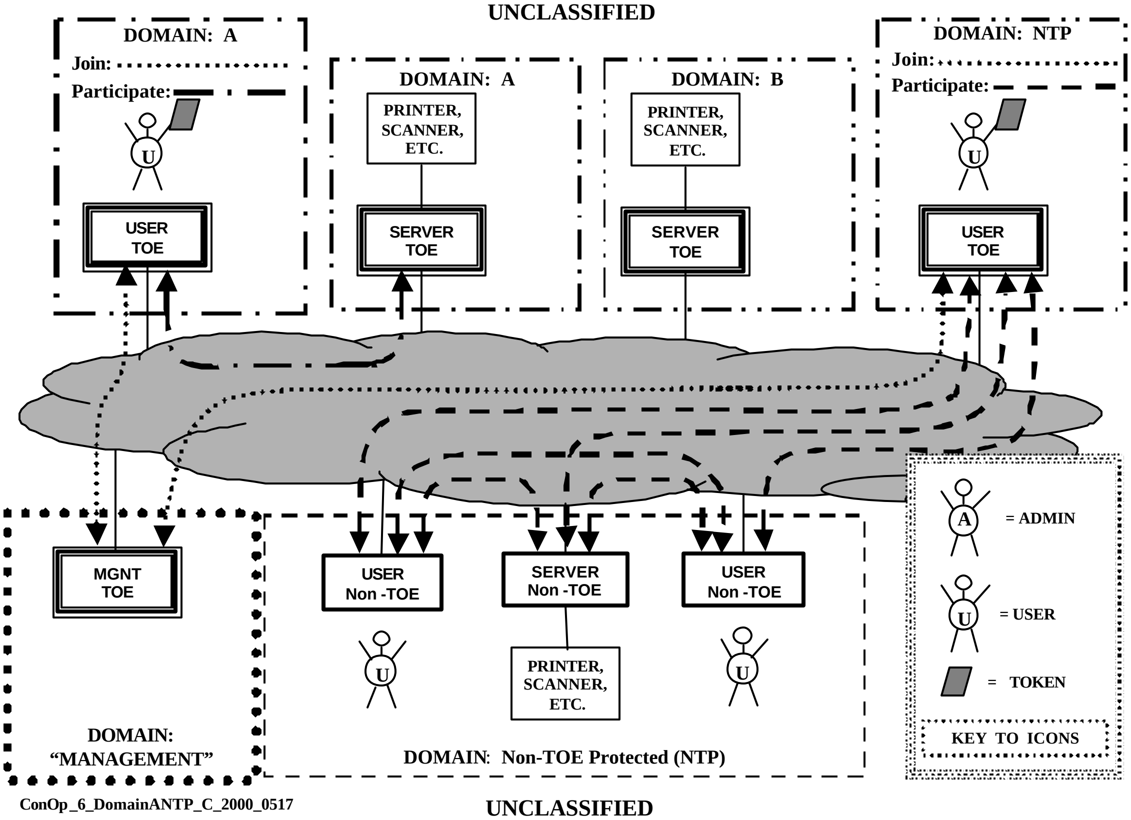


Figure A-7: Upper Left User in Domain "A" & Upper Right User in Domain "NTP."

Figure A-7 depicts the operation of users in two of the three potential domains used in this set of scenarios.

This scenario is provided to emphasize that a User at a TOE, such as the Upper Right TOE, must follow and satisfy the full set of TOE enforced access requirements in order to join the Non-TOE Protected (NTP) domain. Once participating in this NTP Domain, the User at the Upper Right TOE may interact with those Users of the NTP domain at regular workstations and servers, with which his TOE is authorized to participate. When a TOE is interacting with hosts in the NTP Domain, it applies no encryption service.

Requirements for the User at the Upper Left User TOE, who has joined Domain "A", are as they were in the previous scenarios

Appendix B Acronyms

CC	Common Criteria
COTS	Commercial off the Shelf
DIFP	Domain Information Flow Policy
DPA	Domain Participation Authentication
DPAP	Domain Participation Authentication Policy
DoD	Department of Defense
EAL	Evaluation Assurance Level
EKMS	Electronic Key Management System
IT	Information Technology
LAN	Local Area Network
MDS	Multiple Domain Solution
MLS	Multi-Level Security
N/A	Not Applicable
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
O/S	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SPM	Security Policy Model
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
UK	United Kingdom
US	United States

VPN	Virtual Private Network
WAN	Wide Area Network

Appendix C References

Common Criteria for Information Technology Security Evaluation; Part 2: Security Functional Requirements, CCIMB-99-032, v2.1, August 1999.

Common Criteria for Information Technology Security Evaluation; Part 3: Security Assurance Requirements, CCIMB-99-033, v2.1, August 1999